UNIÃO EDUCACIONAL DE BRASÍLIA – UNEB
INOVA EDUCACIONAL
CURSO DE PÓS-GRADUAÇÃO
HABILITAÇÃO EM TECNOLOGIA DE SEGURANÇA DA INFORMAÇÃO

MELHORES PRÁTICAS DE SEGURANÇA EM SERVIÇO VOIP

Carlos Magno Moura Alves Fernandes

Brasília – DF
2011

Carlos Magno Moura Alves Fernandes

MELHORES PRÁTICAS DE SEGURANÇA EM SERVIÇO VOIP

Esta Monografia é apresentada como requisito para obtenção do Certificado de Pós Graduação em Tecnologia de Segurança da Informação pela Instituição UNEB – União Educacional de Brasília/DF.
Especialização em Tecnologia de Segurança da Informação.
Orientador: Prof. Thiago Britto – Mestrando em TI
Co-orientador: Elvio de Souza

Brasília – DF
2011

MELHORES PRÁTICAS DE SEGURANÇA EM SERVIÇO VOIP

Fernandes, Carlos Magno Moura Alves
Pós-Graduação em Tecnologia de Segurança da Informação / Carlos Magno Moura Alves Fernandes
Brasília. União Educacional de Brasília UNEB, 2011
Monografia com o requisito para obtenção do Certificado de Pós-Graduação em Segurança da Informação
Orientador: Prof. Thiago Britto - Mestrando em TI
Co-orientador: Elvio de Souza

Carlos Magno Moura Alves Fernandes

MELHORES PRÁTICAS DE SEGURANÇA EM SERVIÇO VOIP

Monografia aprovada como requisito final para obtenção do Certificado de Pós-Graduação no curso de Tecnologia de Segurança da Informação da União Educacional de Brasília / DF - UNEB.
Especialização em Tecnologia de Segurança da Informação

Data de aprovação

_____/ _____/_____

BANCA EXAMINADORA

Nome:
Instituição:
Assinatura:

Nome:
Instituição:
Assinatura:

Nome:
Instituição:
Assinatura:

Agradecimento

Agradeço a Deus, pela coragem e saúde que tem me dado durante todos os dias de minha vida, aos meus pais, por tudo o que fizeram por mim, pela educação que me permitiram ter, pelas pessoas de caráter, honestidade e humildade que são e que assim me ensinaram a ser.

A minha esposa, ***Evanete Jacobina***, pelo carinho, amor e compreensão em todos os momentos e aos meus filhos que muitas vezes ficaram me esperando pacientemente todos os dias que fui para a faculdade.

Aos amigos da pós-graduação, que colaboram pacientemente comigo e pela amizade e incentivo constantes.

Aos mestres, pela orientação e dedicação.

E a todos os demais que contribuíram, direta ou indiretamente, para a realização desta Monografia.

Frase

...Quanto mais conhecimentos conseguirmos acumular, mais entendemos que ainda falta muito para aprender. É por isso que sofremos...

(Brendon, Randolph, 2011)

Resumo

Nessa monografia são abordados alguns aspectos teóricos e técnicos sobre a tecnologia em serviço VOIP, como: conceitos, diversas técnicas de voz empregadas, os pontos relevantes da rede de transporte para o tráfego de voz digitalizada, tipos de protocolos utilizados, implementações, transporte de voz sobre IP, a diferença entre soluções VOIP com protocolos H323 e SIP, tecnologias VOIP, telefonia IP, equipamentos de VOZ sobre IP, bilhetagem, mecanismos de segurança, propostas de segurança em serviço VOIP e as Melhores Práticas de Segurança em Serviço VOIP.

Além disso, o objetivo é mostrar uma proposta de segurança em serviço VOIP como ideal para a Administração Pública, fonte: Siemens, (2011). Como adquirir de um Servidor Central de Comunicação e Gateways de Voz sobre IP para compor solução de integração de um Sistema de Telefonia de órgãos e entidades da Administração Pública.

Segundo a revista RTI, número 123, 2010, o uso de Voz sobre IP (VOIP) é uma das grandes metas de investimentos para os chamados fornecedores de soluções e para os usuários de telecomunicações nos últimos anos. A tecnologia VOIP, abre um novo horizonte para as possíveis aplicações de integração de voz e dados num mesmo equipamento terminal de usuário, aproxima pessoas geograficamente distantes, aumenta a interatividade de aplicativos e diminui os custos de comunicação quando comparada às convencionais ligações telefônicas interurbanas e internacionais.

Por fim, é uma chance mostrar nessa monografia as Melhores Práticas de Segurança em Serviço VOIP, a satisfação é o elemento motivador na pesquisa de conceitos e novas soluções, que poderão servir como fonte de pesquisa para futuros alunos de Segurança da Informação.

Palavras-Chave: VOZ, VOIP, IP, H323 e SIP.

Abstract

This monograph presents some theoretical and technical aspects of the technology in VOIP service, as concepts, different voice techniques employed, the relevant points of the transmission system for digitized voice traffic, types of protocols used, implementations, voice transport over IP, the difference between VOIP solutions with SIP and H323 protocols, technologies, VOIP, IP telephony, Voice over IP equipment, ticketing, security mechanisms, security proposals in VOIP service and the best practices for VOIP service.

Moreover, the goal is to show a proposal for security in VOIP service as ideal for Public Administration. How to buy a Central Server Communications and Voice over IP Gateways for integration solution composed of a Phone System bodies and entities of public administration.

According to the magazine RTI, Number 123, 2010, the use of Voice over IP (VoIP) is a major investment targets for so-called solution providers and users of telecommunications in recent years. VOIP technology, opens new horizons for the possible applications integrating voice and data in the same user terminal equipment, brings together people geographically distant, increasing the interactivity of applications and reduce communication costs when compared to conventional telephone calls and international calls .

Finally, it is a chance to show in this monograph the Best Practices in Segurity VOIP Service, satisfaction is the motivating factor in the search for new solutions and concepts that can serve as a resource for future students of Information Security.

Keywords: Voice, VOIP, IP, SIP and H323.

Sumário

1. Introdução

Sabe-se que o desenvolvimento tecnológico presente nos equipamentos de informação e de infraestrutura de redes de voz e dados vem cumprindo satisfatoriamente a comunicação das empresas. No entanto os transportes de voz e de dados trafegam em redes independentes, cada uma com suas características próprias.

Em qualquer atividade do ser humano é imprescindível à comunicação, a informação exerce um papel fundamental na vida em coletividade, o homem é um ser em evolução e consequentemente aperfeiçoa o uso da forma de se comunicar. A troca de informação idealiza, concretiza o desenvolvimento tecnológico e promove grandes avanços nessa área que, de fato, é um direcionador fundamental para inovação, resultando no progresso da sociedade.

Segundo a revista RTI, nº 123,(2010), informa que a convergência das telecomunicações, permitirá não só o uso da comunicação fixa como também será possível à mobilidade de forma a beneficiar não só empregados e parceiros, como clientes de forma geral. No entanto, para atender um mercado cada vez mais exigente, a convergência necessita ser escalonável, segura, econômica e capaz de fornecer qualidade de serviço.

Portanto, a referida tecnologia VOIP é sem dúvida o principal caminho para uma comunicação por pacote e motivação para empreendimentos futuros, pois é possível aproveitar o emprego dos telefones celulares, PDAs e laptops para o uso da comunicação, permitindo a mobilidade wireless em um ambiente corporativo, (RTI, nº 123, 2010).

Esclarece-se que a segurança da informação e a qualidade de serviços também serão objetos de estudo nesta monografia. Por fim, uma proposta de segurança de serviço VOIP será otimizada e mostrada nesta monografia, tomando como base algumas referências de estrutura VOIP**.**

1.1. Objetivo

Como muitas das novas tecnologias, o sistema VOIP apresenta novos riscos de segurança e novas oportunidades de ataques. As características inerentes à de rede de dados e telefonia faz do sistema VOIP uma ferramenta suscetível aos problemas de segurança de ambas tecnologias. Além disso, existem os problemas de segurança intrínsecos da tecnologia VOIP, conforme informa a revista RTI, nº 123, (2010).

Portanto, o objetivo é mostrar conceitos, características e as Melhores Práticas de Segurança em Serviço VOIP. Saber que os erros mais comuns quando se avalia a segurança em VOIP é tratar a tecnologia e a sua utilização como outra qualquer.

Desta forma, implementar as medidas de segurança clássicas de um ambiente de comunicação de dados caracteriza a falta de expertise e padrão de segurança especializada, já que VOIP não é somente mais uma aplicação ativa sobre a infraestrutura IP, como são os casos de correio eletrônico e serviços web, onde serão mostrados.

A revista RTI, (2009) me ajudou a entender sobre a tecnologia VOIP, ela afirma que o serviço VOIP é um serviço complexo, que funciona em tempo real, e que, portanto, necessita de cuidados especiais de segurança. Então, para todos que pesquisarem este trabalho, possam se utilizar de uma proposta para ativar um serviço VOIP, tanto em empresas de grande e médio porte.

Portanto, por fim, uma proposta de segurança em serviço VOIP como ideal para a Administração Pública, empresas de grande e médio porte. A aquisição de um Servidor Central de Comunicação e Gateways de Voz sobre IP para compor solução de integração do sistema de telefonia de órgãos e entidades da Administração Pública é fundamental para garantia de um bom funcionamento de um sistema VOIP.

2. Conceitos

2.1. O que é um Sistema de VOIP

Certamente já ouviu falar e até cogitou usar a tecnologia VOIP, seja para fugir das restrições de operadoras de telefonia tradicional, seja para conversar com contatos aqui no Brasil ou no exterior. Os fornecedores do serviço de Tecnologia VOIP são geralmente conhecidas como provedoras, e os protocolos usados para transportar os sinais de voz em uma rede IP são geralmente chamados protocolos VOIP.

Existe uma redução de custo devido ao uso de uma única rede para carregar dados e voz, especialmente no qual os utilizadores já possuem uma rede com capacidade de poder transportar dados VOIP sem custo adicional. A sigla **VOIP** significa *Voice Over Internet Protocol* (Voz sobre Protocolo de Internet), a tecnologia que permite converter o sinal de áudio analógico, como o que temos no telefone comum, em dados digitais, que podem ser transmitidos através de seu computador pela Internet.

O serviço VOIP pode facilitar tarefas difíceis em redes tradicionais. Chamadas entrantes podem ser automaticamente roteadas para o telefone VOIP, independentemente da localização na rede. Por exemplo, é possível levar um telefone VOIP para uma viagem, e onde conectá-lo à Internet pode-se receber ligações, contanto que a conexão seja rápida e estável o suficiente.

O fato de a tecnologia ser atrelada à Internet também traz a vantagem de poder integrar telefones VOIP a outros serviços como conversação de vídeo, mensageiros instantâneos, compartilhamento de arquivos e gerenciamento de listas telefônicas. Estar relacionado à Internet também significa que o custo da chamada independe da localização e dos horários de utilização, ambos os parâmetros usados na cobrança na telefonia fixa e móvel, e cujos valores variam de operadora a operadora.

Vários pacotes de serviço VOIP incluem funcionalidades, que em redes tradicionais seriam cobradas à parte, como conferência a três, redirecionamento de chamadas, rediscagem automática e identificador de chamadas, segundo a revista RTI, (2010).

2.2. Redes - Definição

O termo genérico “rede” define um conjunto de entidades (objetos, pessoas, etc.) interligados uns aos outros. Uma rede permite assim circularem elementos materiais ou imateriais entre cada uma destas entidades, de acordo com regras bem definidas.

Rede (*em inglês network*): Conjunto dos computadores e periféricos conectados uns aos outro. Note que dois computadores conectados constituem por si só uma rede mínima.

Instalação (*em inglês networking*): instalação dos instrumentos e das tarefas que permitem ligar computadores para que possam partilhar recursos em rede.

A seguir uma breve noção dos tipos de redes, que o sistema VOIP pode usar.

2.3. Rede IP

A figura 2, conforme Eric Anderson, (2009), apresenta uma rede IP, formada por três redes interligadas através de roteadores. Roteadores são os dispositivos que recebem os pacotes de dados de um computador em uma rede e os encaminham para outro computador ou roteador na outra rede.

A figura 2, segundo Anderson, Eric (2009), mostra uma rede IP com serviço VOIP.

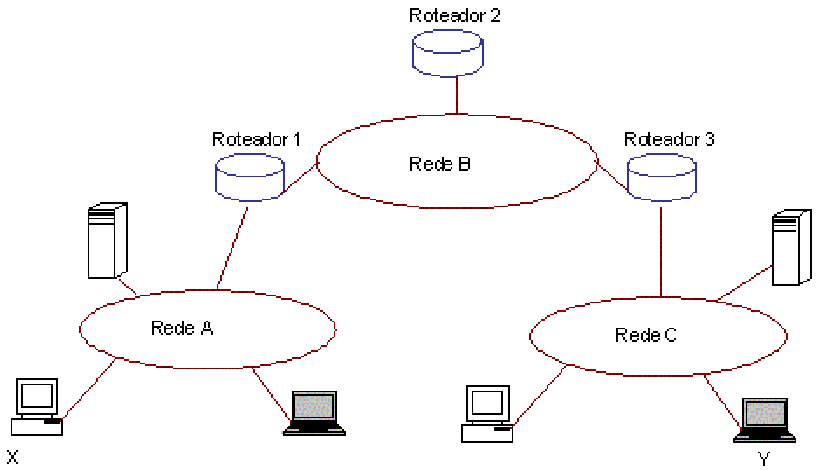

Figura 2 – Rede IP – Fonte: Anderson, Eric (2009)

Um computador X pode enviar pacotes de dados para computadores na sua rede ou para outras redes através do roteador 1.

Na comunicação entre dois computadores os pacotes de dados são processados e encaminhados um a um e de forma independente. Não é estabelecido uma conexão ou circuito virtual que defina um caminho predeterminado para os pacotes.

Dois pacotes enviados pelo computador X podem seguir caminhos diferentes até o computador Y. Podem, por exemplo, passar pelo roteador 1 e ir direto para o roteador 3, ou passar pelos roteadores 1, 2 e 3.

Podem chegar também em ordem diferente da de envio. A Internet é uma rede IP, mas nem toda rede IP faz parte da Internet. Com o crescimento da Internet existe uma tendência para que o IP se torne o protocolo dominante das redes da próxima geração (*Next Generation Network – NGN*) que forneceria inclusive serviços de voz (Voz sobre IP – VOIP).

Garantir a qualidade de serviço na Internet com eficiência é difícil, segundo Anderson, Eric (2009). O protocolo IP permite a atribuição de prioridades aos pacotes mas não existe garantia que estas prioridades serão respeitadas quando se passa de um sistema autônomo para outro.

Estes mecanismos podem ser no entanto implementados no âmbito de uma rede IP sob uma única administração. No próximo item você vai encontrar informações sobre Rede IP sem fio para testar seu entendimento.

2.4. Rede IP Sem Fio

Segundo Anderson, Eric (2009) pode ser muito útil à possibilidade de usar um computador sem o incômodo de ter um cabo de rede conectado o tempo todo. Sugere-se o *FreeBSD* que pode ser usado como um cliente sem fio e até mesmo como um “ ponto de acesso" sem fio. O *FreeBSD* é um sistema operacional livre do tipo Unix descendente do BSD desenvolvido pela Universidade de Berkeley.

2.4.1 Modos de Operação Sem Fio

Há duas formas diferentes de configurar dispositivos sem fio 802.11: BSS e IBSS.

2.4.1.1. Modo BSS

O modo BSS é o modo tipicamente utilizado. O modo BSS é também chamado de modo infraestrutura. Neste modo, uma quantidade de pontos de acesso sem fio está conectada a uma rede cabeada. Cada rede sem fio tem seu próprio nome. Este nome é chamado SSID da rede.

Clientes sem fio conectam-se a estes pontos de acesso. O padrão IEEE 802.11 define o protocolo que redes sem fio usam para conexões. Um cliente sem fio pode ser ligado a uma rede específica, quando um SSID é configurado.

Um cliente sem fio também pode conectar-se a qualquer rede desde que não configure explicitamente um SSID.

2.4.1.2. Modo IBSS

O modo IBSS, também chamado modo ad-hoc, é projetado para conexões ponto-a-ponto. Existem, de fato, dois tipos de modo ad-hoc. Um é o modo IBSS, também chamado de *ad-hoc* ou modo *ad-hoc* do IEEE. O IBSS é definido pelos padrões IEEE 802.11. O segundo o site Wikipédia, (2010), o modo IBSS é também chamado modo ad-hoc demo ou modo *ad-hoc* da Lucent (e, às vezes, confusamente, modo ad-hoc).

Pontos de acesso tipicamente possuem múltiplas conexões de rede: o cartão sem fio e um ou mais adaptadores Ethernet para conexão ao resto da rede. Pontos de acesso podem ser comprados montados ou você pode construir o seu próprio com *FreeBSD* e um cartão sem fio suportado.

Pontos de acesso são dispositivos de rede sem fio que permitem um ou mais clientes sem fio utilizar o dispositivo como um concentrador central. Se usar um ponto de acesso, todos os clientes comunicam-se através destes pontos de acesso. Múltiplos

pontos de acesso são frequentemente usados para cobrir uma área completa como uma casa, negócio ou parque, com uma rede sem fio.

Diversos fornecedores fazem pontos de acesso sem fio e cartões sem fio com características variadas.

3. Protocolo TCP/IP

Quando se fala de protocolo TCP/IP é importante comentar sobre modelo de referência ISO/OSI.

3.1 Modelo de Referência ISO/OSI

Dentro deste cenário de grande variedade de sistemas operacionais, CPUs, interfaces de rede, tecnologias e várias outras variáveis, e a necessidade de interconexão entre os diversos sistemas computacionais, em 1977, a *International Organization for Standardization*-ISO, criou um subcomitê para o desenvolvimento de padrões de comunicação para promover a interoperabilidade entre as diversas plataformas. Foi então desenvolvido o modelo de referência Open Systems Interconnection-OSI.

É importante observar que o modelo OSI é simplesmente um modelo que especifica as funções a serem implementadas pelos diversos fabricantes em suas redes. Este modelo não detalha como estas funções devem ser implementadas, deixando isto para que cada empresa/organização tenha liberdade para desenvolver.

O comitê ISO assumiu o método “dividir para conquistar”, dividindo o processo complexo de comunicação em pequenas subtarefas (camadas), de maneira que os problemas passem a ser mais fáceis de tratar e as subtarefas melhor otimizadas.

O modelo ISO/OSI é constituído por sete camadas, descritas sucintamente a seguir:

7ª Aplicação

A camada de Aplicação, funciona como uma interface de ligação entre os processos de comunicação de rede e as aplicações utilizadas pelo usuário.

6ª Apresentação

Na camada de Apresentação, os dados são convertidos e garantidos em um formato universal.

5ª Sessão

A camada de Sessão, estabelece e encerra os enlaces de comunicação.

4ª Transporte

A camada de Transporte, efetua os processos de sequenciamento e, em alguns casos, confirmação de recebimento dos pacotes de dados.

3ª Rede

A camada de Rede, trata do roteamento dos dados através da rede é implementado aqui.

2ª Enlace

A camada de Enlace, trata da informação e é formatada em quadros (*frames*). Um quadro representa a exata estrutura dos dados fisicamente transmitidos através do fio ou outro meio.

1ª Física

A camada física, define a conexão física entre o sistema computacional e a rede. Especifica o conector, a pinagem, níveis de tensão, dimensões físicas, características mecânicas e elétricas.

Cada camada se comunica com sua semelhante em outro computador. Quando a informação é passada de uma camada para outra inferior, um cabeçalho é adicionado aos dados para indicar de onde a informação vem e para onde vai. O bloco de cabeçalho mais os dados de uma camada é o dado da próxima camada. Observe a figura 3 que esquematiza isto, conforme coleta de dados no CBPF-NT-004, (2000).

A figura 3, mostra as camadas do modelo ISO/OSI.

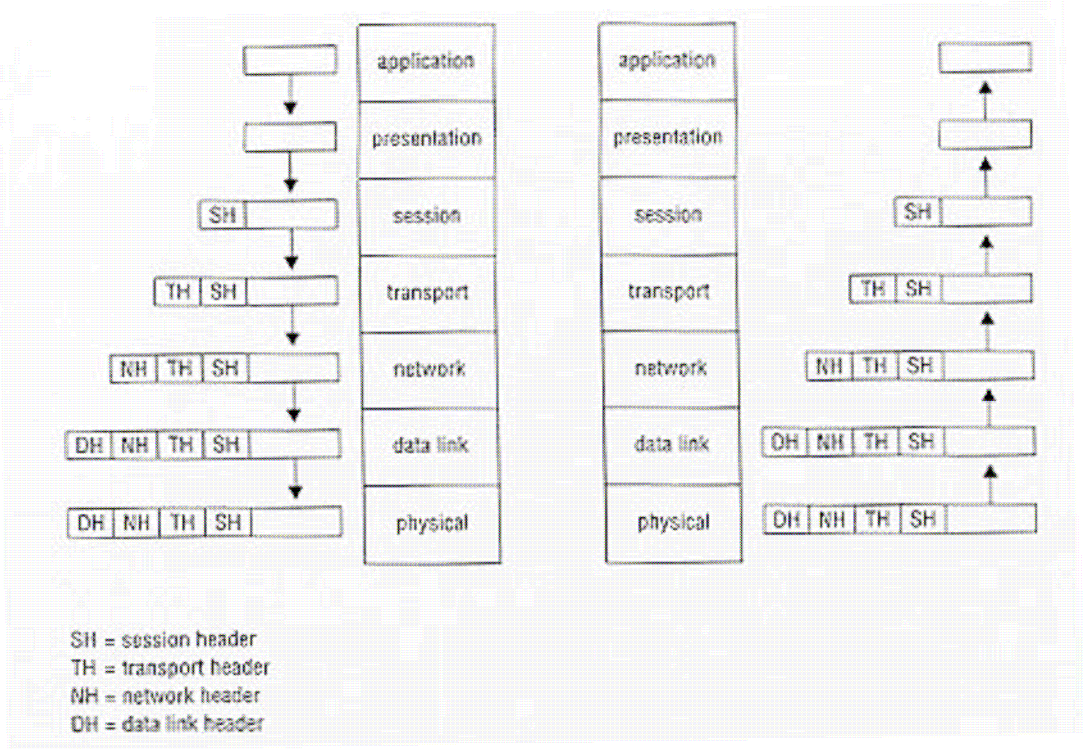

Figura 3 - Camadas do modelo ISO/OSI. Fonte: CBPF-NT-004, (2000)

A unidade de informação muda de nome ao longo das camadas de maneira que podemos saber sobre qual camada se está referindo pelo nome destas unidades. Conforme mencionado nas descrições da figura 3, onde relaciona os diversos nomes destas unidades de informação ao longo das camadas.

4. Telefonia IP

Conforme Alessandro Paganuchi, 2008, a telefonia IP pode ser considerada uma das maiores inovações para telecomunicação telefônica, pois permitem realizar a comunicação de voz em tempo real, unificando o meio de comunicação de tal forma que os sinais de voz e de dados são transmitidos e recebidos simultaneamente, via interconexão unificada, em uma rede de computadores, baseada na arquitetura para Internet.

A figura 4, permite visualizar como é um telefone IP, conforme afirma Alessandro Paganuchi, (2008).

Figura 4 - Telefone IP. Fonte: Alessandro Paganuchi, (2008)

Mas, os protocolos fundamentais da rede IP, TCP, UDP, não são suficientes para satisfazerem as necessidades operacionais básicas da telefonia VOIP, como: sinalização, controle de chamadas e tráfego de voz. Assim, foram desenvolvidos protocolos de comunicação com o objetivo de ser tornar possível a comunicabilidade da chamada de voz em redes IP.

Dessa forma, para que o referido processo de comunicação aconteça são utilizados essencialmente dois protocolos internacionais de comunicação na telefonia IP: O padrão H.323 é parte da família de recomendações da ITU-T (*International Telecommunications Union*), frequentemente utilizados em muitos equipamentos e softwares VOIP; e o SIP, indicado pela IETF (*Internet Engineering Task Force*), o qual, apesar do curto período no processo de padronização, este tem mobilizado muitos produtores da área da telefonia e dados, devido à sua flexibilidade e adesão a padrões legitimamente de internet e de arquitetura aberta.

> *A questão é que, embora o SIP seja um padrão de futuro promissor para interconexão de infraestruturas de comunicação baseada em IP, o H323 é uma tecnologia mais prática, desenvolvida e comprovada neste momento. Fonte: Alessandro Paganuchi, (2008).*

Com uso do VOIP, as chamadas de voz são convertidas em formato digital de tal forma que pode ser transmitido via rede IP, ou seja, pela Internet, intranet privada ou

uma VPN. Basicamente para que o sinal analógico seja convertido para sinal digital e trafegue no meio IP ele deverá sofrer o processo de digitalização.

Este processo requer no mínimo, quatro etapas: a filtragem, a amostragem, a quantização e a codificação. Só assim após o referido processo sinal poderá ser transportado em pacotes IP e transmitido na rede de computadores.

4.1. Telefonia IP Sem Fio

Em uma central privada convencional, uma rede interna ao órgão ou instalada em uma operadora de serviços de telecomunicações mantém sua infraestrutura de voz dados preparadas com uso de cabo metálico ou fibra óptica. Com o VOIP as ligações analógicas são convertidas primeiramente em digital e depois é transmitida por uma rede IP, internet, intranet ou VPN. O conteúdo analógico da transmissão pode ser transformada em VOIP via gateway e trafegadas sobre a internet.

Caso seja uma transmissão externa, o conteúdo VOIP pode trafegar via tronco até um gateway remoto que se encontra em uma central pública que são equipadas pelas operadoras de telefonia.

As chamadas VOIP sem fio também são transmitidas sobre a internet, mas elas dependem do acesso sem fio, que pode ser realizada com a tecnologia baseada em *WiMAX*.

> *A tecnologia VOIP utiliza o protocolo IP para a transmissão de dados através de pacotes em redes IP. Assim, o VOIP consegue alcançar redes internet, intranets e Lans. O sinal de voz (analógico) é digitalizado, sofre compressão e é transformado em pacotes IP e são transmitidos na Rede. Para que esse processo aconteça, são utilizados diversos padrões sendo os mais destacados o H.323 e o SIP. Fonte: Alessandro Paganuchi, (2008).*

No sistema de telefonia IP é utilizado o protocolo TCP/IP (*Transport Control Protocol/Internet Protocol*). Do início até o fim das chamadas, fazem o controle de

banda passante, tradução de endereços, autenticação de chamadas e localização do usuário, esses elementos compartilham os protocolos de transporte de voz.

Segundo a revista RTI (2009), o gateway é utilizado para a conversão de chamadas analógica para digital, em um formato transportável por meio da internet, via RTP (*Real Time Transportation Protocol*), é uma solução em aplicações que abrangem o uso da voz.

Devido a esta característica, seu funcionamento é acoplado a outro protocolo, o RTCP (*Real Time Control Protocol*), este é responsável pela compressão dos pacotes de dados e também atua em seu monitoramento. Consequentemente, na recepção o formato consiste em ser reconduzido para o sinal analógico, sofrendo o processo inverso da digitalização.

A chamada VOIP é capaz de ser aplicada com qualquer combinação, consistem no uso de telefones tradicionais, aparelhos IP e PCs equipados para VOIP, conforme a revista RTI (2009) afirma.

4.2. Integração entre IP

Entretanto, nesse mundo tecnológico composto por tantas siglas, Voz Sobre IP (VOIP) e Telefonia IP podem ser facilmente confundidas. Porém, entre as duas existe um universo composto por cabos, fios e computadores, que as tornam semelhantes, mas não iguais.

4.2.1. A Integração

Segundo a Sisco, (2009), afirmar que existem alguns aplicativos (*SoftPhone)*, é um deles, permitem que o usuário opere um telefone IP a partir de um computador. Neste contexto e como forma de agilizar, ainda mais, a forma como podemos estabelecer uma chamada telefônica desenvolvemos uma automatização que permite iniciar uma chamada telefônica "clicando" unicamente no símbolo como esse (☎), que surge junto do número VOIP na página pessoal de cada utilizador.

E também é possível estabelecer uma ligação telefônica "ligando" para o *login* do utilizador (endereço SIP) que é disponibilizado no sistema escolhido.

4.2.2. O Período de Transição

Para usuários que querem testar os benefícios da Telefonia IP antes de optar pela conversão completa, existem formas de utilizar centrais híbridas, que suportam aparelhos convencionais e IP. Desta forma, a transição se torna mais suave, e os usuários podem optar por utilizar a nova tecnologia apenas em áreas ou aplicações onde os benefícios valeriam o investimento adicional.

5. Equipamentos de Capacitação de VOZ sobre IP

5.1.Grandstream HT 286

O Grandstream HT 286 é um Adaptador VOIP com uma única interface Ethernet e uma saída para telefone convencional que permite que você use seu aparelho de telefone convencional como um Telefone IP. Suporta uma linha VOIP. Perfeito se você já possuir um *Router* Portátil.

A figura 5, mostra um modelo de Adaptador VOIP. Fonte: voipequipamentos, (2010).

Figura 5 - Modelo de Adaptador VOIP – única interface ethernet. Fonte: voipequipamentos, (2010)

5.2. Linksys PAP 2T

O *Linksys* PAP2T é de fácil instalação, portátil e conecta facilmente 2 telefones convencionais a um *Router/switch* na rede já existente na sua casa ou escritório. Suporta duas linhas VOIP. Perfeito se você já possuir um *Router* Portátil.

Conforme figura 6, ela mostra o Linkesys PAP2T, especificado acima.

Figura 6 - Adaptador VOIP para 2 linhas. Fonte: voipequipamentos, (2010)

5.3. Linksys SPA 2102

Linksys SPA 2102 é fácil de instalar e simples de usar. Inclui a funcionalidade de *Router* e permite-lhe conectar telefones convencionais à rede de sua casa ou escritório. Suporta duas linhas VOIP. Inclui funcionalidade de *Router*, conecta até dois computadores. A figura 7, mostra um adaptador VOIP.

Figura 7 - Adaptador VOIP para 2 linhas. Fonte: voipequipamentos, (2010)

5.4. Linksys SPA 8000

O Gateway Digital VOIP *Linksys* SPA 8000 de 8 Linhas é um adaptador VOIP (ATA) completo para pequenas e médias empresas utilizarem serviços de telecomunicações através de sua conexão de internet banda larga. As oito saídas RJ11 para aparelhos de telefone convencionais ou Fax. Um conector *multiport* RJ-21 50. Uma interface Ethernet 10/100 Base-T RJ-45.

Chamada em espera, cancelamento de chamadas, identificador de chamadas e muito mais, a figura 8, mostra um Gateway Digital VOIP de 8 Portas.

Figura 8 - Gateway Digital VOIP de 8 Portas. Fonte: voipequipamentos, (2010)

5.5. Linksys SPA 3102

O Adaptador VOIP SPA3102, traz funcionalidade de adaptador VOIP encontradas no SPA2002 e SPA1001 com um recurso adicional de uma integração total com seu sistema de telefone convencional e aplicativos "*hop-on, hop-off*".

Fornece uma saída RJ-11 para telefonia convencional FXS e uma saída para telefonia convencional FXO. Inclui duas interfaces Ethernet 100 *BaseT* RJ-45 gerenciamento e distribuição de Larga Escala.

A figura 9, mostra um Adaptador VOIP com *Router Linksys*.

Figura 9 - Adaptador VOIP com *Router Linksys*. Fonte: voipequipamentos, (2010)

5.6. Linksys SPA 941

Conecta-se diretamente a um Provedor de Telefonia pela Internet ou a um PABX IP Porta de Ethernet com chave única comutadora, viva-voz, identificador de chamada, chamada em espera, e muito mais Fácil instalação. Configuração através de Menu ou pela web. A figura 10, aponta como é um telefone IP e suas características.

A figura 10, mostra um telefone IP, capaz de fazer até programações para o sistema VOIP.

Figura 10 - Telefone IP. Fonte: voipequipamentos, (2010)

5.7. Ficheiro VOIP

A figura 11, segundo site teleco, (2009), mostra um tipo de ficheiro VOIP com características particulares.

Figura 11 - Ficheiro VOIP - Fonte: Teleco, (2009)

Segundo o site Teleco, (2009) são características particulares deste ficheiro:

- partilhar – copiar, distribuir e transmitir a obra;
- recombinar – criar obras derivadas.

De acordo com as seguinte condição:

- Atribuição – Tem de atribuir a autoria da obra, da forma especificada pelo seu autor ou licenciante.

Entretanto, apesar de amplamente utilizado através de computadores, o VOIP, pode ser utilizado através de adaptadores para telefones analógicos ou gateways VOIP, que são aparelhos que podem se conectar diretamente em uma conexão banda larga e a um aparelho telefônico comum ou a um PABX em posições de troncos ou ramais. Eles fornecem a interligação entre as redes IP e fixas.

5.8. Funcionamento de Trafego em Serviço VOIP

O funcionamento consiste em digitalizar a voz em pacotes de dados para que trafegue pela rede IP e converter em voz novamente em seu destino.

Segue passo a passo um caso de uso de uma ligação.

- O utilizador retira o telefone IP do gancho, e nesse momento é emitido um sinal para a aplicação sinalizadora do roteador de "telefone fora do gancho".
- A parte de aplicação emite um sinal de discagem. O utilizador digita o número de destino, cujos dígitos são acumulados e armazenados pela aplicação da sessão.
- Os gateways comparam os dígitos acumulados com os números programados; quando há uma coincidência ele mapeia o endereço discado com o IP do gateway de destino.
- A aplicação de sessão roda o protocolo de sessão sobre o IP, para estabelecer um canal de transmissão e recepção para cada direção através da rede IP. Se a ligação estiver sendo realizada por um PABX, o gateway troca a sinalização analógica digital com o PABX, informando o estado da ligação. Se o número de destino atender a ligação, é estabelecido um fluxo RTP sobre UDP entre o gateway de origem e destino, tornando a conversação possível.

Quando qualquer das extremidades da chamada desligar, a sessão é encerrada.

6. Dispositivos VOIP

As comunicações unificadas e o VOIP wireless prometiam contribuir para melhorar os diversos campos, no entanto, a implementação está a ser prejudicada por uma abordagem fragmentada.

Conforme a revista redação oficina da net, (2008), a mobilidade, acesso sem fio e convergência são as palavras de ordem no atual mercado das redes de comunicação. Trata-se de uma tendência irreversível, que vem se tornando realidade e incorporando-se ao mundo das tecnologias.

6.1. Outros Dispositivos VOIP

A transmissão de voz em redes sem fio pode não ser uma coisa nova em termos tecnológicos, mas, sem dúvida, é algo novo em termos de serviço. Até pouco tempo, às redes tradicionais de telefonia, o serviço de transmissão de voz vem se tornando uma solução viável no ambiente das redes sem fio das empresas e mesmo nas residências.

Para que a voz seja transmitida através de uma rede de computadores, ela deve ser transformada para o formato digital (bits) e enviada na forma de pacotes. Logo passa a ser vista como "informação" e não mais como "voz". Esse conceito, adaptado à realidade das redes sem fio, herda todas as vantagens e problemas que qualquer transmissão de dados teria, uma vez que não existe qualquer distinção entre ambos os tráfegos (pacotes de voz ou de dados).

Quando essa técnica de transmissão é introduzida sobre uma solução sem fio, os aspectos tecnológicos observados são basicamente os mesmos que já existem para a rede antes destinada ao tráfego exclusivo de dados, uma vez que, na prática, é o transporte da voz (no formato digital) utiliza um protocolo específico (neste caso, o protocolo IP) e apresenta os mesmos mecanismos e funcionalidades quando são transportados apenas dados.

6.2. Exposição e ameaças

Por se tratar de uma tecnologia que utiliza a infraestrutura de uma rede sem fio, é natural pressupor que esta afirmativa seja fundamentada e que o tráfego de voz implique realmente em novos riscos quando abordamos os aspectos de segurança para uma rede de computadores.

> *À medida que a utilização de voz cresce em uma rede, também crescerá a exposição dessa rede às ameaças de segurança. Fonte: Revista de Oficina Net, (2008).*

Todavia, devemos observar que, se uma rede sem fio segue regras de segurança eficientes para a transmissão das informações, o tráfego de dados é seguro e o de voz também o será, pois, como os canais de comunicação são os mesmos, a voz herda a

segurança que a rede sem fio oferece para os dados. Entretanto, se a rede sem fio não oferece nenhum meio de proteção para a informação digital, as transmissões de sinais de voz também não terão qualquer tipo de segurança.

Por exemplo, segundo Rodrigo Teles, (2010), o conceito de *Hotspot*, que numa tradução livre do inglês pode significar ponto quente, ponto de acesso ou ponto de extensão, pode referir-se a várias áreas: Exemplos de *hotspot* : 1) *Hotspot wi-fi*; 2) *Hotspot* geologia; 3) *Hotspot*.

Portanto, no caso dos *hotspots* que oferecem acesso sem fio à Internet livremente e sem oferecer qualquer nível de segurança, tanto dados quanto voz estarão sujeitos aos vários tipos de riscos e ataques encontrados nesse ambiente inseguro. Cabe ao usuário do serviço providenciar garantias quanto à privacidade de suas comunicações, estabelecendo políticas de acesso capazes de oferecer segurança para a informação que deseja transmitir.

Na verdade, a união entre voz e redes sem fio não traz ameaças novas ou que não possam ser combatidas com políticas de segurança eficientes, embora essa associação possa, certamente, aumentar os efeitos das vulnerabilidades da rede por várias razões.

Por exemplo, segundo a revista oficina net, (2008), é comum um administrador de rede buscar formas alternativas de prover aos seus usuários funcionalidades de rede adicionais (telefonia, por exemplo).

Neste aspecto, a segurança deve tornar-se um dos fatores e característica mais importante dos serviços disponibilizados, sendo que as funcionalidades oferecidas devem considerar a aplicação de políticas de segurança que sejam integradas e capazes de abranger a totalidade de rede.

6.3. Central Privada de Comutação

A Central Privada de Comutação Telefônica (CPCT) consiste no processo de comutação por circuito. É uma central de comunicação telefônica automática, de uso reservado, conhecida por *Private Automatic Branch Exchange* (PABX*)*, que tem como principal objetivo a transmissão de voz, a ininterrupção da transmissão, garantia e

confiabilidade no tráfego da comunicação e ainda provê o aumento da produtividade dos usuários e supervisiona as ligações dentro de um âmbito privado, além do mais, concentra diversos ramais e proporciona um conjunto de facilidades e serviços e para tanto, não oferece custos nas ligações interna (entre ramais), pois, as chamadas não trafegam pela operadora de telefonia.

Segundo o site Rodrigo Telles, (2010), numa CPCT a voz é comutada automaticamente e transmitida sobre o meio de comunicação (fio de cobre, fibra óptica, rádio frequência) por uma operadora que presta serviços de telefonia. As conexões entre as centrais públicas e privadas são realizadas por circuitos conhecido como tronco que é responsável pela comunicação entre o meio interno da empresa com a infraestrutura externa de comunicação pública de voz.

No Brasil o circuito tronco utiliza o recomendado pela a ITU-T, feixe E1 de 2 Mbps, podendo ser unidirecionais (entrada ou saída) ou bidirecionais (entrada e saída). O meio de transmissão da voz pode ser, cabo coaxial, fibra óptica ou rádio - frequência.

O PABX IP é um equipamento privado para comutação telefônica que emprega a tecnologia de voz sobre IP e realiza chamadas telefônicas sobre as redes de dados IP como se estivesse utilizando a rede de telefonia tradicional. Para tanto, a comunicação sofre a conversão do sinal analógico para digital, são transmitidas como pacotes de dados em conjunto com a rede de computadores, abrange funcionalidades avançadas do tradicional processo de comunicação.

Além disso, O PABX IP é apropriado para se conectar com os troncos da rede pública de forma a prover a comunicabilidade entre dois pontos utilizando a central pública, ou seja, interliga as ligações interna ao usuário externo de telefonia.

Portanto, o PABX IP realiza comutação por pacotes das ligações com as mesmas facilidades ou ainda melhores aos dos serviços do PABX tradicional e ainda suportam novos benefícios que reúnem uma série de aproveitamento de Internet, intranet e telefonia e ainda permite que os ramais aproveitem as linhas para chamadas externa de forma transparente para os usuários dos serviços de telefonia.

7. Protocolos

Segundo o esccritor Rodrigo Telles, (2010), o conceito mais próximo de protocolo, é o conjunto de regras sobre o modo como se dará a comunicação entre as partes envolvidas. Protocolo é a "língua" dos computadores, ou seja, uma espécie de idioma que segue normas e padrões determinados. É através dos protocolos que é possível a comunicação entre um ou mais computadores. Os protocolos de rede nasceram da necessidade de conectar equipamentos de fornecedores distintos, executando sistemas distintos, sem ter que escrever a cada caso programas específicos

A estrutura que sofre uma conexão VOIP normalmente compreende um conjunto de composições de sinalização entre os pontos envolvidos no processo de comunicação pontos-finais (*gateways, gatekeepers*), pois, para o estabelecimento da conexão, é necessário determinar o ponto de origem e de destino, ou seja, roteamento entre os pontos.

Além disso, existem métodos de sinalização que são usados basicamente no sistema de telefonia como, identificação do número chamador e do número chamado, sinalização acústica (campainha, tons: de discagem, de desconexão, de ocupado, de chamada), tempo de espera e tempo de conversa.

Para tanto, ainda existem diferentes protocolos de comunicação desenvolvidos para serem utilizados pela tecnologia VOIP, com propósito de atender de forma transparente e com qualidade o uso da comunicação de voz unificada com a rede da dados.

7.1. Protocolo H 323

O protocolo H.323 constitui uma das bases da tecnologia de voz sobre IP. Segundo o site gta/voip/protocolos, (2010), o H.323 demarca comunicações multimídia, como dados, áudio e vídeos, em tempo real, isto se dá através de pacotes-base da rede (como o IP-base de rede), portanto, faz parte da família ITU-T (*International Telecommunication Union Telecommunication Standardization sector*), pertencente a série H que está ligada a Sistemas Audiovisuais e Multimídia.

É especificado pelo ITU que em 1996 tenha sido lançada a primeira versão do H-323, focando principalmente as comunicações multimídias em ambiente LAN, não garantindo a QoS (qualidade de serviço). Paralelamente ao dado lançamento, experimentos de comunicações de voz pela Internet realizavam-se. Alguns produtos linearizados ao estabelecimento de chamadas, baseados na compressão do tráfego de voz, surgiram; porém, devido a falta de um padrão, nasciam incompatíveis entre si.

Desta forma, logo viu a necessidade da criação do padrão VOIP, adotando-se também o H-323, a segunda versão do H-323 desenvolveu-se impulsionada pelo surgimento e uso de comunicações entre PC's (baseado em tefefones) e telefones tradicionais e entre PC's (pela internet), sendo efetivamente lançada em 1998 pelo ITU. Esta nova versão foi também adaptada a ambientes WAN e MAN (*metropolitan area network*), deixando de ser adequada somente a ambiente LAN.

Esta versão trouxe melhorias no quesito segurança, além de uma otimização do tempo para liberação do canal depois da chamada ter chegado ao seu destino. Deve-se mencionar também a maior integração com a recomendação T.120 (Protocolos de dados para conferência multimídia).

A versão 3 do protocolo H-323 foi lançada em 1999 com novas utilidades tais como fax, maior rapidez no estabelecimento de chamadas além de comunicações entre *gatekeepers*. Este, por sua vez, muitas vezes age como um interruptor virtual, sendo sempre o ponto central para as chamadas dentro da zona e provendo serviços de controle de chamada para estações registradas. Além disso, recorreu-se a reutilização de conexões, controle remoto de dispositivos além de incluir um tipo de *endpoint* (tecnologia de imagens) simplificado.

Pode-se definir o protocolo H.323 como sendo um conjunto de especificações que foi esquematizado para receber à estrutura de transporte IP, desenvolvida pela ITU-T, que é uma série de protocolos para padronizar um modelo de comunicação de multimídia utilizando rede baseada em pacotes para conexão entre dispositivos de áudio e ou vídeo, operando na camada de transporte.

Portanto, o protocolo H323, pode ser usado sobre qualquer rede, o protocolo TCP/IP tem como principal objetivo a comunicação de multimídia em tempo real. A

flexibilidade oferecida é uma das principais características do H.323, pois, admite não só a aplicação de comunicação de voz, como também, vídeo conferência e multimídia.

7.2. Protocolo SIP

O Protocolo SIP teve origem em meados da década de 1990, para que fosse possível adicionar ou remover participantes dinamicamente numa sessão *multicast*. O desenvolvimento do SIP concentrou-se em ter um impacto tão significativo quanto o protocolo HTTP, a tecnologia por trás das páginas da web que permitem que uma página com links clicáveis conecte-se com textos, áudio, vídeo e outras páginas da web.

Enquanto o HTTP efetua essa integração através de uma página web, o SIP integra diversos conteúdos a sessões de administração. O SIP recebeu uma adoção rápida como padrão para comunicações integradas e aplicações que usam presença. (Presença significa a aplicação estar consciente da sua localização e disponibilidade).

Segundo o site UFRJ, (2010), o protocolo SIP é um protocolo de sinalização para chamadas telefônicas baseada em rede IP e vem se tornando um padrão das comunicações VOIP. Está sendo utilizado como padrão de sinalização e controle de chamadas entre terminais VOIP, pois, foi projetado especificamente para a Internet, desenvolvido pelo IETF.

Segundo a UFRJ, tecnologia, (2010), o protocolo SIP, devido a sua arquitetura utilizada que é similar a outros protocolos tradicionais como HTTP e SMTP, que são baseadas somente em texto. O SIP é um protocolo de sinalização da camada de aplicação. Utiliza como suporte o protocolo (UDP) não orientado a conexão para o tráfego dos pacotes de voz.

Proporcionam ainda, serviços adicionais, tais como identificação de chamada, transferência, redirecionamento de chamadas, autenticação de chamadas, conferência, desvio de chamada, tecla de atalho. Permite, ainda, a aplicação de benefício inteligente para rede telefônica, além disso, é utilizado para originar, incorporar e finalizar chamadas em processo de comunicação com um ou mais participantes, teleconferência.

7.2.1. Arquitetura do SIP

Segundo a UFRJ, Tecnologia, (2010), os principais componentes da arquitetura do protocolo SIP são:

7.2.1.1. Agente do Utilizador

O Agente do Utilizador é o terminal SIP ou o software de estação final. O Agente do Utilizador funciona como um cliente no pedido de inicialização de sessão e também age como um servidor quando responde a um pedido de sessão. Dessa forma, a arquitetura básica é cliente/servidor.

O Agente do Utilizador é "inteligente", com isso ele armazena e gerencia situações de chamada. O Agente do utilizador faz chamadas com um endereço parecido com o de e-mail ou número de telefone (E.164).

Exemplo: SIP:user@proxy.university.edu

Isso faz URLs SIP fáceis de associar com o endereço de e-mail do usuário. O Agente do Utilizador pode aceitar e receber chamadas de outro agente do utilizador sem requerer nenhum componente adicional do SIP. Os componentes restantes fornecem gerenciamento e funcionalidades adicionais.

7.2.1.2. Servidor Proxy SIP

Um tipo de servidor intermediário do SIP é um Servidor Proxy SIP. O Servidor Proxy SIP encaminha pedidos antes do Agente do utilizador para o próximo servidor SIP retendo também informações com a finalidade de poderem ser usadas para fins de contabilidade e ou de fatura.

Além disso, o servidor proxy SIP pode operar com comunicação *stateful* (por exemplo, como um circuito, TCP) ou *stateless* (por exemplo como um UDP). O servidor *SIP stateful* pode "dividir" chamadas por ordem de chegada para que várias extensões que estejam a tocar todos ao mesmo tempo sendo que a primeira a atender ficará com a chamada.

Essa capacidade significa que se pode especificar que um telefone de desktop SIP, um telefone celular SIP e aplicações de videoconferência de casa SIP possam sinalizar simultaneamente quando estiver a receber uma chamada. Ao atender um dos dispositivos e iniciada a conversação, os restantes param de sinalizar.

O servidor *proxy* SIP pode utilizar múltiplos métodos para tentar resolver o pedido de endereço de host, incluindo busca de DNS, busca em base de dados ou retransmitir o pedido para o "próximo" servidor *proxy*.

7.2.1.3. Servidor de Redirecionamento SIP

Outro tipo de servidor intermediário do SIP é o Servidor de Redirecionamento SIP. A função do servidor de redirecionamento SIP é fornecer a resolução de nome e localização do usuário. O servidor de redirecionamento SIP responde ao pedido do Agente do Usuário fornecendo informações sobre o endereço do servidor para que o cliente possa contatar o endereço diretamente.

7.2.1.4. Registrador

O Registrador SIP fornece um serviço de informação de localidades; ele recebe informações do Agente do Usuário e armazena essa informação de registro. A arquitectura do SIP faz uso do SDP (*Session Description Protocol*). O SDP foi uma ferramenta de conferência *multicast* via IP desenvolvida para descrever sessões de áudio, vídeo e multimídia. Na realidade, qualquer tipo de MIME (*Multipurpose Internet Mail Extension*) pode ser descrita, similar à habilidade do e-mail de suportar todos os tipos de anexos em mensagens. A descrição da sessão pode ser usada para negociar uma aceitação de um conjunto de tipos de mídias compatíveis.

Como resultado dessa arquitetura, o endereço do usuário SIP remoto é sempre o mesmo (por exemplo sip:user@proxy.univ.edu), mas ao invés de estar amarrado a um endereço estático, ele comporta-se como um endereço dinâmico que reflete a localização atual do destinatário. A combinação de Proxy e Servidor Redirecionador dá ao SIP grande flexibilidade de arquitetura; o usuário pode empregar vários esquemas

simultaneamente para usuários localizados e é o que faz a arquitetura do SIP ser bem adaptada para suportar mobilidades.

Mesmo quando o usuário remoto é móvel, o Proxy e o redirecionador podem ser usados para passar adiante o pedido de conexão para o usuário da locação atual. As sessões podem envolver múltiplos participantes, de forma similar a uma chamada multiponto H.323.

Comunicações dentro de uma sessão em grupo podem ser via *multicast* ou via uma rede de chamadas *unicast*, ou até mesmo uma combinação dos dois. Um outro resultado da arquitetura do SIP é a sua adequação natural como um ambiente de colaboração devido às suas habilidades de apresentar múltiplos tipos de dados, aplicações, multimídia, etc. com uma ou mais pessoas.

7.3. Protocolo de Transporte

Aplicações utilizadas na internet usam TCP/IP, enquanto VOIP usa RTP/UDP/IP. O Protocolo de Controle de Transmissão (TCP) é um protocolo da camada 4 (quatro) orientado a conexão e confiável, pois, garante que os segmentos entregues sejam confirmados e ainda proporciona a retransmissão de quaisquer segmentos que não foram confirmados, coloca os seguimentos na sequência correta no destino e oferece a prevenção e controle de congestionamento.

Porém, o TCP não é um protocolo usual para aplicação em tempo real como exemplo, o uso e aproveitamento da comunicação por voz, visto que as características de sua arquitetura provocam atraso excessivo (latência) dificultando o controle de *jitter*.

Por outro lado, o UDP (*User Datagram Protocol*) é um protocolo de transporte não orientado à conexão, sua finalidade principal consiste em expor datagramas da camada aplicação. Ele, também, não garante nem a ordem, nem a correção e nem a integridade dos pacotes, que podem chegar corrompidos ou simplesmente não chegar, além disso, não usa janela, nem confirmação, assim, caso seja necessário a confiabilidade, este, é fornecida exclusivamente por protocolos da camada superior, aplicação.

O UDP é projetado para aplicações que não precisam juntar sequência de segmentos. Enquanto o TCP tem a finalidade de deixar a comunicação confiável, a intenção do UDP é ser ágil. Assim sendo O UDP por si só não realiza muito e emprega uma estrutura de cabeçalho simples.

7.4. Protocolo de Transporte em Tempo Real

O Protocolo de Transporte em Tempo Real, *Real-time Transport Protocol*, (RTP) é utilizado em aplicações de tempo real, responsável pela transmissão e determina um formato de pacote padrão para o envio de áudio pela Internet. E ainda, estabelece a forma de fragmentação do tráfego de dados, incluí a cada fragmento informação de sequência e de tempo de entrega.

Podemos também dizer segundo o site lee.eng, (2010) é definido como 1) Definido na RFC 1889; 2) Normalmente usado sobre o UDP. Este protocolo fornece serviços de: 1) Identificação do tipo de carga útil (mídia); 2) Números de sequência; 3) Estampa de tempo. Este protocolo não possui: 1) Controle de fluxo; 2) Controle de erros; 3) Confirmação; 4) Mecanismo de solicitação de retransmissões.

7.5. Protocolo de Controle de Transporte em Tempo Real

Quanto ao controle, é realizado pelo Protocolo de Controle de Transporte em Tempo Real, *Real Time Control Protocol*, (RTCP), funciona em conjunto com o RTP. Deste modo, o RTP realiza a entrega dos dados, enquanto RTCP envia pacotes periódicos de controle aos usuários da conexão, o qual tem como função principal o fornecimento do reenvio da qualidade dos serviços oferecidos pelo RTP.

Para tanto, os protocolos RTP/RTCP aproveitam o UDP como protocolo de transporte, os dois são definidos pela RFC 3550 do IETF (*Internet Engineering Task Force*). Segundo o site lee.eng, (2010): 1) É também definido na RFC 1889; 2) Possui pacotes RTCP enviados em *multicast* contém relatórios de remetente e/ou receptor com dados estatísticos; 3) O remetente pode mudar a taxa de transmissão; 4) O destinatário pode sincronizar diferentes fluxos de mídias em uma sessão RTP.

8. Bilhetagem

8.1. Bilhetagem ou Call Detail Register (CDR).

Segundo a revista RTI, (2010), a bilhetagem ou *Call Detail Register* (CDR), são soluções inovadoras para administração e relatórios de bilhetagem VOIP. Acredita-se que o diferencial esteja nos recursos para manipulação dos clientes e possibilidade de customizações para atender de maneira personalizada as diversas formas de trabalho VOIP. se tratando de bilhetagem, esse processo é definido como o processo no sistema telefônico que permite a aquisição e gravação de informação sobre as chamadas, isto como método de segurança.

No processo de bilhetagem, a central telefônica também emite um bilhete onde consta o local da chamada, quem originou a chamada, quem recebeu a chamada, o tempo de início da chamada, o tempo de término, etc. As informações da bilhetagem podem ser impressos.

A central telefônica pode estar conectada a um computador para controle de bilhetagem. Para se ter a mesma bilhetagem entre CPCT e STFC deverá ocorrer sincronismo entre as mesmas, como por exemplo, sincronismo do relógio entroncamento digital é a interligação entre Centrais Telefônicas, através de um sistema digital de transmissão. O termo *Tie-Line* é usado para referenciar um entroncamento proprietário (link privado).

9. Mecanismos de Segurança

Geralmente são considerados os seguintes atributos de segurança para redes de comunicação. Estes constituem o conjunto de características que o sistema de segurança deve conferir a rede, que são:

9.1. A Disponibilidade

A Disponibilidade refere-se a sobrevivência da rede mesmo sob ataque de impedimento de Serviço ou Operação lançado sobre alguma das camadas do sistema.

9.2. A Confiabilidade

A Confidencialidade assegura que certo tipo de informação não seja descoberta por entidades não autorizadas. Confidencialidade é a propriedade da informação pela qual não estará disponível ou divulgada a indivíduos, entidades ou processos sem a autorização.

9.3. A Integridade

A Integridade deve garantir que uma mensagem não é corrompida quando transferida na rede a não ser por falha na interface de rádio, mas nunca por comportamento malicioso de um nó.

9.4. A Autenticação

A Autenticação deve capacitar os nós de confirmar a identidade de seus pares de comunicação, evitando tentativas de mascaramento e personificação por nós mal intencionados.

9.5. O Não-Repúdio

O Não-Repúdio confere ao sistema a capacidade de sempre identificar a origem de uma mensagem, o que é muito útil quando da necessidade de detectar nós comprometidos.

10. Tipos de Ataques em Serviços VOIP

Segundo o Sisco, Voip, (2009), os tipos de ataque tidos como os mais realizados no campo da tecnologia VOIP serão mostrados aqui. Os ataques ao VOIP podem ser divididos em quatro categorias, segundo o tipo principal de impacto: 1) De disponibilidade; 2) De integridade; 3) De confidencialidade e 4) De privacidade.

Os ataques à disponibilidade podem causar perda de receita, de produtividade e incremento dos custos (normalmente decorrentes de manutenções não previstas) pela indisponibilidade ou degradação do serviço.

Na Internet a comunicação é feita através de fluxo de pacotes de dados. Mas, segundo a logicengenharia, (2010), o que acontece quando uma máquina emissora envia mais dados do que a máquina destino consegue lidar?

A máquina destino irá recusar os novos pacotes, pois ela possui uma enorme quantidade de informação para processar e, portanto, ficará indisponível. Por isso esse ataque ganhou o nome de *Denial Of Services* (DoS) que em português significa Negação De Serviços.

Já o *Distributed Denial Of Services* (DDoS) que em português significa Negação De Serviços Distribuída, é mais potente. Um cracker invade vários servidores e instala um programa para ataques DoS em cada um deles, fazendo dos mesmos máquinas zumbis. Do computador central, o cracker envia um comando e os Zumbis começam a enviar o máximo de pacotes ao alvo fazendo um ataque sincronizado.

Como ele utiliza muitos zumbis o ataque fica muito mais eficiente e dificilmente a vítima não cai. Embora para o ataque se concretizar não seja preciso que a máquina caia, ele apenas deve deixá-la lenta o suficiente para que o cliente abandone o serviço.

Esses ataques ganharam mais importância entre os administradores de redes quando foram usados em grandes sites como a UOL e Yahoo entre outros. Dentro dessa categoria incluem-se ataques como o DoS e DDoS.

Os ataques à integridade tentam comprometer os serviços VOIP através de troca de identidade e outras atividades fraudulentas. Ataques deste tipo podem ter impacto financeiro, prejudicar a reputação, deixar vazar informação sensitiva e causar perda de produtividade. Dentro dessa categoria podemos incluir MITM, *Call Hijack, Spoofing, Call Fraud, Phishing e Malware*.

Exemplos de ataque à privacidade e confidencialidade consistem na escuta (*eavesdropping*), que tem o impacto de expor informações confidenciais de determinado negócio, operação ou pessoa física, podendo evoluir para um ataque à integridade;

assim como o SPIT onde mensagens não autorizadas são recebidas, violando a privacidade dos usuários do serviço.

A lista de ataques possíveis é muito vasta. Também são sumarizados alguns destes ataques, apenas para que o leitor tenha uma visão do tipo de abuso que pode ser implementado:

10.1. SIP Bombing

O SIP *bombing* é um ataque tipo DOS (*Denial of Service*), no qual uma grande quantidade de mensagens VOIP modificadas são "bombardeadas" contra algum dos componente da rede SIP. Nesse caso o sistema fica ocupado tratando essas mensagens e o serviço fica indisponível ou com a qualidade degradada;

10.2. SIP Cancel/Bye DoS

Outro ataque tipo DOS, no qual o atacante simula uma mensagem de desconexão do tipo CANCEL ou BYE (dependendo do estado da chamada) evitando que o originador possa iniciar conversações ou derrubando sessões em andamento;

10.3. Manipulação dos registros

A Manipulação dos registros é um ataque tipo *Spoofing* que pode evoluir para *Call Fraud* e MITM, onde um *user agent* se faz passar por outro, podendo receber suas chamadas ou fazer chamadas no seu nome;

10.4. Falsificação de 3xx Response Codes

A falsificação de 3xx Response Codes, é um ataque tipo *Spoofing* que pode evoluir para *Call Hijack* ou MITM, onde uma mensagem de redirecionamento do tipo 3xx é forjada de forma que o originador transmita a sua comunicação através de um componente de rede comprometido;

10.5. Escuta do RTP

A escuta do RTP utiliza CODEC's padrão para codificar a voz. Se o invasor consegue capturar o tráfego RTP de um canal de voz (facilitado pelo uso das redes wireless), é muito fácil remontar e ter acesso à conversa sendo conduzida;

10.6. Manipulações do SSRC no RTP

A manipulações do SSRC no RTP é um ataque do tipo *Spoofing* que pode evoluir para um DoS, *Call Hijack ou Call Fraud*, a reescrita do SSRC pode ser utilizada para interromper chamadas ou remover um usuário da chamada, tomando o seu lugar, ou para enviar conteúdo falso.

10.7. Manipulação do CODEC no RTP

A manipulação do CODEC no RTP é o ataque do tipo DOS, no qual o atacante pode degradar a qualidade da conversa mudando sistematicamente o CODEC sendo usado, por exemplo, para um CODEC de mais alto consumo de banda.

10.8. Inserções RTCP

As inserções RTCP é o taque do tipo DOS, através do qual o atacante pode interromper conversações em andamento falsificando mensagens do protocolo de controle do RTP, por exemplo mensagens do tipo BYE.

10.9. Appliance Hacking

A *Appliace Hackin*g é o tipo de ataque onde os equipamentos são gerenciados inadequadamente.

11. Tipos de Defesas em Serviço VOIP

A tecnologia VOIP apresenta desafios de segurança. Uma ligação de VOIP tem duas partes: as mensagens de sinalização que configuram a chamada e o fluxo de mídia

que carrega a “voz”. Os caminhos de sinalização e de mídia são separados, exigindo conexões lógicas entre as duas partes se comunicando através de VOIP.

Portanto, conforme mencionado no item 1.1, a segurança não é fator motivador para serviço VOIP, mas as comunicações de voz não protegidas podem ser interceptadas, e roubadas ou corrompidas. Pacotes de voz não comutados podem ser encontrados e monitorados em tempo real. Telefones que utilizam software para converter um PC em um telefone de IP, estes são vulneráveis a monitoração se o PC estiver infectado com um cavalo de Tróia que monitore o tráfego da LAN.

O VOIP expõe as comunicações de voz aos mesmos tipos de ameaças de segurança aos quais as comunicações de dados estão expostas. As redes VOIP são consideradas alvo importante por hackers, já que é possível capturar informações sigilosas (como administrativas, financeiras ou estratégias de mercado), cuja utilização indevida poderia causar danos irreparáveis para uma empresa.

Portanto, um fator relevante sobre a segurança da tecnologia VOIP é a escolha de equipamentos de qualidade e infraestrutura bem planejada, focadas numa boa qualidade de serviço e prevendo o combate a ataques que porventura aparecerem.

11.1. Dificuldades com Serviço VOIP

Como o UDP não fornece um mecanismo para assegurar que os pacotes de dados sejam entregues em ordem sequencial, ou ainda que forneça garantias de qualidade de serviço, as implementações VOIP sofrem com o problema de latência e *jitter* (variações de atraso). Esse problema é acentuado quando uma conexão por satélite é usada, devido ao grande atraso de propagação (entre 400 e 600 milissegundos para um satélite geoestacionário). O nó receptor deve reestruturar os pacotes IP que podem estar fora de ordem, atrasados ou desaparecidos, enquanto assegura o fluxo de áudio.

Outro desafio para o roteamento de tráfego VOIP são os firewalls e os tradutores de endereço. O *Skype* utiliza um protocolo proprietário para rotear chamadas entre utilizadores *Skype*, permitindo atravessar NAT e firewall.

Outros métodos para passar *firewalls* incluem STUN e ICE.

Em resumo, os principais desafios técnicos do VOIP são latência, perda de pacotes, eco e segurança. A principal causa de perda de pacotes é o congestionamento, que pode ser controlado por gerenciadores de congestionamento de rede. Causas comuns de eco incluem inconsistências de impedância em circuitos analógicos.

Segundo a revista RTI, (2010), do ponto de vista de gestão, se a estrutura de rede e os equipamentos forem antigos ou inexistentes, uma mudança para VOIP pode custar alto para a aquisição de novos equipamentos como o cabeamento, comutadores, roteadores, telefones IP, e aumento da banda de conexão para suportar essa nova tecnologia.

11.2. Qualidade de Serviço VOIP

As conexões, de banda larga, possuem uma qualidade razoável de transmissão. Quando os pacotes IP são perdidos ou atrasados em algum ponto da rede, existe uma queda momentânea da voz na conversação. Isso é mais perceptível em redes bastante congestionadas ou onde existem grandes distâncias entre os pontos de conexão.

Alguns protocolos já foram definidos para suportar e relatar qualidade de serviço em ligações VOIP, incluindo RTCP XR (RFC3611), SIP RTCP *Summary Reports*, H.460.9 *Annex* B (para H.323), H.248.30 e extensões MGCP.

11.3. Chamadas de Emergência de Serviço VOIP

A natureza do Protocolo de Internet torna difícil a localização geográfica dos utilizadores na rede. Chamadas de emergência portanto não podem ser roteadas facilmente para o centro de chamadas mais próximo, e são impossíveis em alguns sistemas. Entretanto, sistemas VOIP podem rotear chamadas de emergência para linhas de telefone não emergenciais.

O suporte de envio de fax sobre VOIP ainda é limitado. Os codecs de voz existentes não foram desenvolvidos para a transmissão de fax. Um esforço para remediar essa situação é definir uma solução baseada em IP alternativa para oferecer Fax sobre IP, nomeadamente o protocolo T.38.

Outra solução possível é tratar o sistema de fax como um sistema de troca de mensagens que não necessita transmitir em tempo real, assim como enviar um fax como anexo de e-mail ou como uma impressão remota.

A figura 11 mostra um telefone móvel VOIP-WIFI da *BroadVoice*,

Figura 11 - Telefone Móvel. Fonte: voipequipamentos, (2009)

Outra solução possível é tratar o sistema de fax como um sistema de troca de mensagens que não necessita transmitir em tempo real, assim como enviar um fax como anexo de e-mail ou como uma impressão remota.

11.4. Integração em Sistema Global de Número Telefônico

Enquanto redes tradicionais e móveis compartilham um padrão global comum (E.164) que permite alocação e identificação de qualquer linha telefônica,existe padrão similar adotado em redes VOIP. ENUM *(Eletronic Number Mapping)* novo padrão de numeração para o ambiente VOIP em substituição ao padrão de segurança.

As soluções VOIP, ainda não suportam criptografia, o que resulta na possibilidade de se ouvir chamadas alheias ou alterar seu conteúdo. Um método de segurança é disponível através de codificadores de áudio patenteados que não são disponíveis para o público externo, dificultando o entendimento do que está sendo trafegado e protegendo o consumidor.

Entretanto, outras áreas de segurança através de obscuridade não têm tido sucesso a longo prazo devido à grupos de engenharia reversa. Algumas empresas usam compressão de dados para tornar a escuta alheia mais difícil. Entretanto, segurança através de criptografia e autenticação ainda não está amplamente disponível ao público.

11.5. Uso Corporativo

O consumidor corporativo usa a telefonia IP para obter as vantagens da abstração da informação na rede. Com o VOIP é necessário somente fornecer uma conexão de dados e mais banda de rede.

Apesar de poucos ambientes de escritório e residências utilizarem uma infraestrutura puramente de telefonia IP, provedores de telecomunicações usam um tipo de tecnologia, geralmente em uma rede IP dedicada para conectar estações e converte sinais de voz em pacotes IP e vice e versa.

O resultado desta utilização é uma rede digital genérica (tráfego de voz e dados) com escalabilidade. Para efeito de comparação entre os sistemas de telefonia fixa convencional e o sistema de telefonia IP, quanto suas vantagens e desvantagens, estes parâmetros tem os critérios de desempenho de um sistema de comunicação frente aos custos de sua implementação e utilização.

Segundo Medeiros, (2006), o bom desempenho dos sistemas de comunicação relaciona-se com o projeto, qualidade dos equipamentos e desempenho das equipes técnicas de instalação e manutenção. O sistema de comunicação deve atender os requisitos de confiabilidade, qualidade, segurança, rapidez de respostas, flexibilidade e duplicação dos meios; apontados na tabela a seguir.

11.5.1. Vantagens e Desvantagens do Sistema VOIP

No Brasil as políticas regulatórias para telefonia criaram uma série de regras de proteção de território, de tarifas, de concorrência, mas nenhuma delas para trazer real vantagem para o consumidor. Assim, vemos a cada ano as contas telefônicas consumirem uma parcela cada vez maior do orçamento de indivíduos e de empresas.

Além desse crescimento indexado da conta telefônica, há a enorme carga tributária incidente sobre os serviços de telefonia. Pegue sua conta telefônica e veja o total de ICMS incidente. Considere também os impostos indiretos, que as operadoras repassam para a conta dos clientes.

Nesse cenário sombrio, surge uma promessa de luz no fim do túnel para os usuários através da tecnologia de Voz Sobre o Protocolo da Internet, ou Voz Sobre IP, representado pela sigla VOIP.

Soluções gratuitas para chamadas entre computadores, como o popular *Skype*, são muito úteis e permitem falar com alguns contatos usando a conexão à Internet de banda larga. No entanto, esses serviços gratuitos permitem somente chamadas de computador a computador e muitas vezes precisamos chamar um telefone real, fixo ou celular.

Conforme a tabela 1, alguns requisitos de desempenho do sistema precisam ser melhorados, como confiabilidade, qualidade e rapidez, para que se possa atingir o padrão consolidado pela telefonia convencional, com isso não sendo necessário distribuir uma rede específica para a telefonia no ambiente de trabalho. ela mostra os requisitos essenciais para um bom sistema de comunicação.

Conforme relata a revista RTI, (2010), a maior vantagem da implementação da telefonia IP está relacionada à redução dos custos em ligações telefônicas, principalmente nas de longas distâncias, apesar da potencialidade de economia e flexibilidade, as empresas não se encontram preparadas, ainda, para enfrentar os desafios que envolvem a implementação e gerenciamento dessa nova tecnologia.

Tabela 1: Requisitos Essenciais de Sistema de Comunicação. Fonte: Siemens, (2009)

Confiabilidade	**Qualidade**	**Segurança**
Continuidade da comunicação, garantia da efetivação do enlace, garantia de conexão com os usuários de destino e ausência de interrupções. Caso haja interrupção inesperada do sistema, um meio de comunicação paralelo deve assegurar a continuidade das operações de comunicação.	Condições das informações recebidas entre os usuários, medida através da relação sinal/ruído e distorção.	Aplicações de medidas de proteção dos enlaces que visam dificultar o entendimento de informações captadas por terceiros e prevenir possíveis interferências.
Rapidez	**Flexibilidade**	**Duplicação**

Decurso de tempo entre a ação inicial do assinante que inicia o processo de chamada e a efetivação do enlace.	Convergência com outros sistemas com diferentes tipos de sinal, como voz, dados e vídeos.	Possibilidade de ampliação dos meios de comunicação caso haja um aumento de demanda pelo sistema.

Empresas maiores também fazem uso de gateway para as redes tradicionais, reduzindo custos de mão de obra externa. Seu uso é ainda mais visível quando uma empresa necessita comunicar dois sítios distantes a nível internacional.

As aplicações corporativas, sejam eles software cliente ou hardware específico para tal aplicação, disponibilizam formas simples para vários utilizadores (colaboradores das empresas) comunicarem entre si sem que requeiram grandes centrais telefônicas e/ou sequências complexas de números e símbolos no telefone para darem início a uma sessão.

Portanto, nas situações de uso do sistema através de software proprietário do fornecedor de serviço VOIP este poderá disponibilizar outro tipo de ferramentas como transferência de arquivos, partilha de pastas e em alguns casos a partilha do próprio computador.

12. Regulamentação do Serviço VOIP no Brasil

O órgão responsável pela regulamentação de telecomunicações no Brasil é a Agência Nacional de Telecomunicações (ANATEL). Portanto a única regulamentação é da Anatel. Conforme o portal Anatel, (2009).

A ANATEL não regulamenta as tecnologias, mas os serviços de telecomunicações que delas se utilizam. A comunicação de voz utilizando computadores conectados à Internet, uma das aplicações desta tecnologia, é considerada Serviço de Valor Adicionado, não sendo necessária autorização da Anatel para prestá-lo.

Nesse contexto, o uso da tecnologia de VOIP deve ser analisado sob três aspectos principais. Primeiro, a comunicação de voz efetuada entre dois computadores pessoais, utilizando programa específico e recursos de áudio do próprio computador,

com acesso limitado a usuários que possuam tal programa, não constitui serviço de telecomunicações, mas serviço de valor adicionado, conforme entendimento internacional.

Segundo, a comunicação de voz no âmbito restrito de uma rede corporativa ou na rede de uma prestadora de serviços de telecomunicações, de forma transparente para o assinante, efetuada entre equipamentos que podem incluir o aparelho telefônico, é caracterizada como serviço de telecomunicações.

Neste caso, é exigida a autorização para exploração de serviço de telecomunicações para uso próprio ou para prestação a terceiros. Por fim, a comunicação de voz de forma irrestrita com acesso a usuários de outros serviços de telecomunicações e numeração específica (objeto de controle pela Anatel) é caracterizada como serviço de telecomunicações de interesse coletivo.

É imprescindível autorização da Agência e a prestação do serviço deve estar em conformidade com a regulamentação.

13. Gateway

O Gateway ou porta de ligação, é uma máquina intermediária geralmente destinada a interligar redes, separar domínios de colisão, ou mesmo traduzir protocolos. Exemplos de gateway podem ser os *routers* (ou roteadores) e *firewalls*, já que ambos servem de intermediários entre o utilizador e a rede. Um *proxy* também pode ser interpretado como um gateway (embora em outro nível, aquele da camada em que opera), já que serve de intermediário também.

Depreende-se assim que o gateway tenha acesso ao exterior por meio de linhas de transmissão de maior débito, para que não constitua um estrangulamento entre a rede exterior e a rede local. E, neste ponto de vista, estará dotado também de medidas de segurança contra invasões externas, como a utilização de protocolos codificados.

Cabe igualmente ao gateway traduzir e adaptar os pacotes originários da rede local para que estes possam atingir o destinatário, mas também traduzir as respostas e devolvê-las ao par local da comunicação. Assim, é frequente a utilização de protocolos

de tradução de endereços, como o NAT, que é uma das implementações de gateway mais simples.

Note-se, porém, que o gateway opera em camadas baixas do Modelo OSI e que não pode, por isso, interpretar os dados entre aplicações (camadas superiores). No entanto, por meio do uso de heurísticas e outros métodos de detecção de ataques, o gateway pode incorporar alguns mecanismos de defesa. Esta funcionalidade pode ser complementada com um firewall.

14. Nat

Em redes de computadores, NAT, *Network Address Translation*, também conhecido como *masquerading* é uma técnica que consiste em reescrever os endereços IP de origem de um pacote que passam por um *router* ou firewall de maneira que um computador de uma rede interna tenha acesso ao exterior (rede pública).

14.1. Explicação sobre o Nat

Com o surgimento das redes privadas com internet partilhada, surgiu o problema de como os computadores pertencentes à esta rede privada poderiam receber as respostas aos seus pedidos feitos para fora da rede.

Por se tratar de uma rede privada, os números de IP interno da rede (como 10/8, 172.16/12 e 192.168/16) nunca poderiam ser passados para a Internet pois não são roteados nela e o computador que recebesse um pedido com um desses números não saberia para onde enviar a resposta. Sendo assim, os pedidos teriam de ser gerados com um IP global do *router*. Mas quando a resposta chegasse ao *router*, seria preciso saber a qual dos computadores presentes na LAN pertencia à resposta.

A solução encontrada foi fazer um mapeamento baseado no IP interno e na porta local do computador. Com esses dois dados o NAT gera um número de 16 bits usando a tabela *hash*, este número é então escrito no campo da porta de origem.

O pacote enviado para fora leva o IP global do *router* e na porta de origem o número gerado pelo NAT. Desta forma o computador que receber o pedido sabe para onde tem de enviar a resposta. Quando o *router* recebe a resposta faz a operação inversa, procurando na sua tabela uma entrada que corresponda aos bits do campo da porta. Ao encontrar a entrada, é feito o direcionamento para o computador correto dentro da rede privada.

Um computador atrás de um *router* gateway NAT tem um endereço IP dentro de uma gama especial, própria para redes internas. Como tal, ao ascender ao exterior, o gateway seria capaz de encaminhar os seus pacotes para o destino, embora a resposta nunca chegasse, uma vez que os *routers* entre a comunicação não saberiam reencaminhar a resposta (imagine-se que um desses *routers* estava incluído em outra rede privada que, por ventura, usava o mesmo espaço de endereçamento). Duas situações poderiam ocorrer: ou o pacote seria indefinidamente[1] reencaminhado, ou seria encaminhado para uma rede errada e descartado.

Por reconhecer apenas os protocolos TCP e UDP, não é possível estabelecer uma conexão que não utilize um desses protocolos. O número gerado pela tabela de *hash* tem apenas 16 bits, o que faz com que esta técnica permita apenas 65505 conexões ativas. Dependendo das dimensões da rede e do número de pedidos feitos pelos computadores desta rede, o limite de 65505 pode ser facilmente atingido.

14.2. Vantagens sobre o Nat

As entradas no NAT são geradas apenas por pedidos dos computadores de dentro da rede privada. Sendo assim, um pacote que chega ao *router* vindo de fora e que não tenha sido gerado em resposta a um pedido da rede, ele não encontrará nenhuma entrada no NAT e este pacote será automaticamente descartado, não sendo entregue a nenhum computador da rede. Isso impossibilita a entrada de conexões indesejadas e o NAT acaba funcionando como um *firewall*.

15. Roteador

Roteador (estrangeirismo do inglês *router*, ou encaminhador) é um equipamento usado para fazer a comutação de protocolos, a comunicação entre diferentes redes de computadores provendo a comunicação entre computadores distantes entre si.

Roteadores são dispositivos que operam na camada 3 do modelo OSI de referência. A principal característica desses equipamentos é selecionar a rota mais apropriada para encaminhar os pacotes recebidos. Ou seja, escolher o melhor caminho disponível na rede para um determinado destino.

15.1. Funcionalidade do Roteador.

Os roteadores utilizam tabelas de rotas para decidir sobre o encaminhamento de cada pacote de dados recebido. Eles preenchem e fazem a manutenção dessas tabelas executando processos e **protocolos** de atualização de rotas, especificando os endereços e domínios de roteamento, atribuindo e controlando métricas de roteamento.

O administrador pode fazer a configuração estática das rotas para a propagação dos pacotes ou pode configurar o roteador para que este atualize sua tabela de rotas através de processos dinâmicos e automáticos, veja na figura 12 como funciona um roteador.

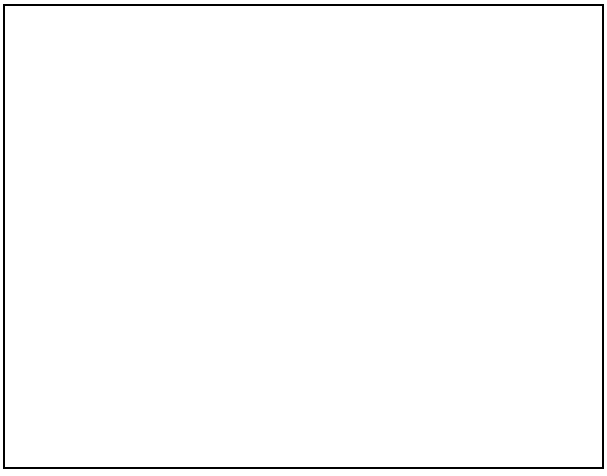

Figura 12 – Roteador. Fonte: Wikipédia, (2009)

Parte interna de um roteador, a saber: **1** eletrônica do telefone (para *ADSL*) **2** *LED* de status da rede **3** LED de status do USB **4** *processador* da *Texas Instruments* **5**

porta *JTAG* de teste e *programação* **6** *memória RAM* de 8 MB **7** *memória flash* **8** regulador da alimentação **9** *fusível* da alimentação principal **10** conector de energia **11** *botão* de reiniciar **12** *cristal de quartzo* **13** porta *ethernet* **14** *transformador* ethernet **15** transmissor e receptor ethernet **16** porta *USB* **17** porta do telefone (*RJ11*) **18** fusível do conector de telefone.

Os roteadores encaminham os pacotes baseando-se nas informações contidas na tabela de roteamento. O problema de configurar rotas estáticas é que, toda vez que houver alteração na rede que possa vir a afetar essa rota, o administrador deve refazer a configuração manualmente, já a obtenção de rotas dinamicamente é diferente, conforme Beraldo, Fabio - Revista TI, 2010.

15.2. Protocolos de Roteamento

Os protocolos de roteamento, são protocolos que servem para trocar informações de construção de uma tabela de roteamento. É importante ressaltar a diferença entre protocolo de roteamento e protocolo roteável.

Protocolo roteável é aquele que fornece informação adequada em seu endereçamento de rede para que seus pacotes sejam roteados, como o TCP/IP e o IPX. Protocolo de roteamento possui mecanismos para o compartilhamento de informações de rotas entre os dispositivos de roteamento de uma rede, permitindo o roteamento dos pacotes de um protocolo roteado. Exemplo de protocolo de roteamento: RIP, OSPF, IGRP , BGP, EGP, etc.

Roteadores modernos de grande porte assemelham-se a centrais telefônicas, e cujo as tecnologias atualmente estão sendo convergidas, e que no futuro os roteadores podem até mesmo substituir por completo.

Um roteador que conecta um cliente à Internet é chamado roteador de ponta. Um roteador que serve exclusivamente para transmitir dados entre outros roteadores (por exemplo, em um provedor de acesso) é chamado um roteador núcleo. Um roteador é usado normalmente para conectar pelo menos duas redes de computadores, mas existe uma variação especial usada para encaminhar pacotes em uma VLAN. Nesse caso, todos os pontos de rede conectados pertencem à mesma rede.

16. Proposta de Implantação de Segurança em Serviço VOIP

16.1. Objetivo

Proposta, (Siemens,2010) apresentado nesta monografia como referência para empresas, na aquisição de Servidor Central de Comunicação e Gateways de Voz sobre IP, para compor solução de integração do Sistema de Telefonia de órgãos e entidades da Administração Pública Federal, é uma demonstração de sugestão onde, compreendendo fornecimento, instalação, ativação, transferência de tecnologia e garantia de funcionamento.

16.2. Especificações Técnica

16.2.1. Item 1: Equipamentos para compor a solução

Previsão de aquisição de 1 (um) Servidor Central de Comunicação para solução de integração do sistema de telefonia dos órgãos e entidades, em conformidade com as especificações técnicas definidas, de forma a implementar todos os serviços e características necessárias ao perfeito funcionamento da solução.

16.2.2. Item 2: Gateway de Voz sobre IP - CLASSE I

Previsão de aquisição de 3 (três) gateways de voz sobre IP de pequeno porte para solução de integração do sistema de telefonia dos órgãos e entidades, em conformidade com as especificações técnicas definidas, de forma a implementar todos os serviços e características necessárias ao perfeito funcionamento da solução.

16.2.3. Item 3: Gateway de Voz sobre IP - CLASSE II

Previsão de aquisição de 10 (dez) gateways de voz sobre IP de pequeno/médio porte para solução de integração do sistema de telefonia dos órgãos e entidades, em conformidade com as especificações técnicas definidas, de forma a implementar todos os serviços e características necessárias ao perfeito funcionamento da solução.

16.2.4. Item 4: Gateway de Voz sobre IP - CLASSE III

Previsão de aquisição de 7 (sete) gateways de voz sobre IP de médio porte para solução de integração do sistema de telefonia dos órgãos e entidades, em conformidade com as especificações técnicas definidas, de forma a implementar todos os serviços e características necessárias ao perfeito funcionamento da solução.

16.2.5. Item 5: Gateway de Voz sobre IP - CLASSE IV

Previsão de aquisição de 10 (dez) gateways de voz sobre IP de médio porte para solução de integração do sistema de telefonia dos órgãos e entidades, em conformidade com as especificações técnicas definidas, de forma a implementar todos os serviços e características necessárias ao perfeito funcionamento da solução.

16.2.6. Item 6: Gateway de Voz sobre IP - CLASSE V

Previsão de aquisição de 3 (três) gateways de voz sobre IP de médio/grande porte para solução de integração do sistema de telefonia dos órgãos e entidades, em conformidade com as especificações técnicas definidas, de forma a implementar todos os serviços e características necessárias ao perfeito funcionamento da solução.

16.3. Especificações da Proposta

16.3.1. Servidor de Comunicação da Central para Voz sobre IP

A configuração do Sistema Central deve permitir o controle e o processamento da capacidade máxima do serviço com todos os gateways previstos neste Edital (8.080 canais SIP, com expansão para 12.120), quer seja na primeira ou na segunda etapa, sem a degradação do serviço. Também deverá ser capaz de realizar a bilhetagem total prevista no sistema (65.000 ramais, com expansão para 100.000). Define-se ramal como identificador único tanto para terminais IPs quanto para cada telefone conectado ao PABX do órgão que se comunica com a Solução de Voz via gateway E1-IP;

O Sistema Central deve atuar como SIP Proxy Server em modo stateful e SIP Registrar Server, conforme RFC 3261, possibilitando o registro de gateways e roteamento de chamadas de qualquer entidade SIP (terminais SIP, gateways de qualquer fabricante, *Asterisk*), independente da informação de Vendedor ID contido no cabeçalho do protocolo SIP;

O Sistema Central deve ser composto de 2 (dois) equipamentos (duas plataformas idênticas e independentes, compostas de hardware, único ou em módulos, e software com suporte do mesmo fabricante) redundantes entre si, em modo Fail Over (caso um equipamento fique inoperante, o outro assume automaticamente, em modo on-line). Os equipamentos deverão permitir a ampliação através da simples adição de módulos, bastidores e cartões, não necessitando da troca de hardware inicial;

Cada equipamento deve possuir, no mínimo, processadores com velocidade total de 2,4 GHz, disco rígido de 6 GBytes, interface de rede tipo Ethernet 10/100 Mbps e ventiladores, todos duplicados e redundantes entre si, em modo Fail Over e *hot-swappable*;

Possuir fontes de alimentação duplicados, redundantes e *hot-swappable* operando em 110 ou 220 VAC de entrada, 60 HZ, fase/neutro/terra, capazes de suportar a capacidade máxima de cartões/módulos dos equipamentos ofertados;

Possuir, para cada equipamento do Sistema Central, alimentação elétrica alternativa (no-breaks) com:

Entradas de alimentação redundantes operando em 110 e 220 VAC automático, 60 HZ, capazes de suportar a capacidade máxima de cartões/módulos dos equipamentos ofertados;

Garantir a continuidade do serviço por um período mínimo de 8 horas, em caso de falha de energia elétrica (em plena carga);

Sinalização visual para modo de fornecimento de energia pela rede elétrica ou bateria;

Sinalização indicativa de fim da carga da bateria;

Proteção contra descarga total das baterias com sinalização antes do desligamento;

Gerar alarmes via SNMP e possibilitar que o no-brake envie notificações destes alarmes a destinatário(s) de Correio Eletrônico (e-mail);

O Sistema Central deverá permitir a interligação de pelo menos 100 PABXs através da rede IP;

Fornecer bastidor tipo rack, possuindo porta frontal com chave e vidro temperado, compatível para instalação e acondicionamento para cada equipamento ofertado;

O Sistema Central deverá possuir controle fim-a-fim de cada chamada terminada na rede de telefonia de longa distancia ou celular, monitorando tanto o estabelecimento como o encerramento da mesma pelo usuário do PABX por traz do gateway (na FASE I), bem como pelo outro usuário da RPT numa operadora de longa distancia ou Celular (na FASE II);

Atender aos seguintes padrões:

IP (Internet Protocol - RFC 0791);

TCP (Transmission Control Protocol - RFC 0793);

UDP (User Datagram Protocol - RFC 0768);

DNS (Domain Name System - RFC 1034);

HTTP (Hypertext Transfer Protocol - RFC 2616);

HTTPS (HTTP over TLS - RFC 2818);

FTP (File Transfer Protocol - RFC 0959) ou TFTP (Trivial File Transfer Protocol - RFC 1350);

ICMP (Internet Control Message Protocol - RFC 0792);

NTP (Network Time Protocol - RFC 1305);

SNMP v2 (Simple Network Management Protocol - RFC 1905) ou superior;

Telnet (RFC 0854);

SIP (Session Initiation Protocol - RFC 3261);

SDP (Session Description Protocol - RFC 2327);

Fazer a comutação inteligente de voz entre dispositivos IP (ramais IP e gateways) sem passar pelo Servidor de Comunicação (peer-to-peer), comutando na CPU apenas o registro e a sinalização e residindo na LAN/WAN todo o tráfego de voz das partes envolvidas;

Prever plano de numeração transparente para o usuário, fazendo com que o Servidor de Comunicação reconheça e indique o devido roteamento das chamadas *saintes* dos PABXs, não alterando a forma de utilização dos usuários;

Conexão com a Rede Pública de Telefonia (RPT):

A conexão com a RPT se dará exclusivamente com a padronização SIP. O tráfego SIP originado num Gateway ou terminal SIP deve ser roteado diretamente em SIP para outro Gateway ou terminal SIP (Fase I), ou para a operadora de em longa distancia ou celular (Fase II) e vice-versa;

O sistema deverá fazer a seleção de rota de menor custo para chamadas de longa distância, incluindo eventuais redes de dados, e chamadas de celular, sem a necessidade de digitar um código de rota especifico;

Possuir total controle nos canais IP (número de conversações simultâneas), de tal modo que, caso todos os canais estejam ocupados, o equipamento fará encaminhamento da chamada pela rede pública, assim não comprometendo a banda disponível e a qualidade de voz das ligações em curso;

O sistema deverá fornecer rotas alternativas em caso de indisponibilidade do destino. Deste modo, caso o sistema detecte que o número de destino se encontra indisponível, ou não se encontra registrado, o mesmo irá encaminhar automaticamente a chamada para RPT, quer seja através do gateway (Fase I) ou diretamente (Fase II);

16.3.2. Redundância

O equipamento deverá possuir redundância, através da duplicação de CPU, memória e disco;

O sistema deverá permitir que a segunda plataforma seja acomodada em localidade diferente, de modo a garantir a sobrevivência do sistema caso o site principal

se torne indisponível ou inacessível. Neste caso, a segunda plataforma deverá controlar toda a carga da rede de forma transparente sem interromper o serviço;

Para proteção dos dados, o sistema deverá ter a habilidade para armazenar (*backup*) e exportar cópias das informações de configuração críticas incluindo informações de autenticação, de forma criptografada;

O equipamento deverá possuir rotinas periódicas de detecção e correção de erros. Caso o erro não possa ser reparado, o sistema deve avisar o administrador automaticamente;

O Sistema deverá gerar os bilhetes (CDRs) que contenha todas as informações necessárias que subsidiem as características requeridas na especificação do tarifador;

Possuir um buffer interno para bilhetes de no mínimo quinze mil bilhetes, visando garantir o armazenamento de bilhetes no caso de falha do sistema de tarifação;

Gerenciamento remoto utilizando protocolo SNMP, por meio de Web Browser ou de aplicativo cliente fornecido pela empresa;

Permitir a implantação de rotas de tráfego para as operadoras celulares de tecnologia GSM e CDMA, utilizando entroncamento com tecnologia SIP.

16.4. Sistema (Software e Hardware) de Gerenciamento, Monitoramento e Manutenção do sistema Central e dos Gateways

A configuração do gerenciador deve permitir o processamento da capacidade máxima do sistema sem degradar o serviço, quer seja na primeira ou na segunda etapa;

O sistema deve permitir a configuração de dados de rotas, e de tabelas de encaminhamento de chamadas.

Possibilitar administração remota através de interface web e linha de comando;

Acesso à interface de administração de sistema deve ser seguro. O sistema deve garantir autenticação para o acesso via rede LAN permitindo no mínimo cinco sessões de administração simultâneas.

Os recursos de gerência deverão permitir o gerenciamento de configuração, de falhas e alarmes, de inventário, de backup e de log de operações, todos de forma gráfica.

O sistema deve possibilitar a monitoração da qualidade das chamadas de voz sobre IP, informando sobre parâmetros de qualidade de serviço na rede (*delay, jitter*, perda de pacotes), possibilitar gerenciamento via SNMP, com *Logs* de eventos e classificação dos traps.

16.4.1. Gerenciamento de Falhas

Possuir gerência de falhas e desempenho, tanto local quanto centralizado, possibilitando o gerenciamento via interface gráfica com alternância de cores e em tempo real;

Possuir alarmes para notificação e localização, como por exemplo, em caso de perda do link com o sistema de tarifação ou com o PABX do órgão, congestionamento de canais SIP e E1, taxa excessiva de perda de chamadas, problema com módulos ou fontes de alimentação;

O alarme deverá ser categorizado, possuir informações como data/hora, local, equipamento e mensagem descritiva do erro, e seus procedimentos deverão ser automatizados (iniciar um backup, enviar um e-mail);

Permitir a identificação e o gerenciamento de falhas, permitindo demonstrar uma visão hierárquica de, no mínimo, 500 ativos de rede (switches, Servidores de Comunicação, gateways), possuindo interface com seus configuradores;

Permitir visualizar o status do dispositivo e assistência para isolamento de problemas;

Relatar histórico de eventos;

Possuir classificação dos dispositivos e configuração de "*thresholds*", possuindo gerenciamento de alarmes para este último, listando todos os componentes que ultrapassaram a linha de um *threshold*;

Permitir a gestão de nível de serviço (SLA), baseado em dados como variações de tempo de resposta, volume e latência.

16.4.2. Gerenciamento de Tarifação do Sistema de Central e dos Gateways

A configuração do tarifador deve permitir o processamento da capacidade máxima do sistema, quer seja na primeira ou na segunda etapa;

Realizar bilhetagem centralizada de todas as ligações estabelecidas e controladas pelo Proxy Server, incluindo as chamadas encaminhadas/recebidas pelo gateway da RPT;

Capacidade de tarifar e bilhetar 65.000 ramais independente de modelo de PABX e local de instalação dos ramais e com capacidade de expansão para até 100.000 ramais;

Possuir discos (HD) para armazenar histórico das informações do tarifador, suficiente para armazenar 24 horas/dia 120 dias, os discos devem utilizar a tecnologia de RAID 1. O sistema deve avisar o percentual de utilização dos discos e permitir o monitoramento de ocupação dos mesmos. Os arquivos com mais de 120 dias serão baixados dos discos para DVD, tudo gerenciado pelo sistema. O sistema deverá possui gravadora de DVD para tanto.

Coletar, custear e organizar todos os dados de chamadas de voz que venham a ser obtidos em toda a Rede;

Fornecer ferramenta que permita a cada usuário e órgão rodar relatórios referentes apenas aos seus próprios dados devido a funcionalidades empregadas de segurança e permissões de acesso, oferecendo recursos que permitam ao usuário filtrar os dados de seu relatório para análise e visualizá-los em formato gráfico para WEB, imprimi-los, enviá-los por e-mail ou salvá-los em arquivos nos formatos (PDF, TXT, XLS e RTF);

Criação de controles de níveis de acesso por usuário (administrador, operador, visualização);

Possuir um mecanismo para recalcular automaticamente todas as cobranças quando alguma das tabelas de preços das operadoras for modificada;

Alocar o custo da chamada ao respectivo usuário, separando a utilização de acordo com o destino da chamada (local, DDD, DDI ou VC1), mantendo sempre as informações da origem física da chamada;

Permitir a implementação de cotas de consumo/limites por usuário, com licença irrestrita e independente da quantidade de usuários;

Possuir aplicativo de identificação automática de ligações particulares dos usuários via interface web;

Serviço de tarifação automática, uma vez que o bilhete (CDR) for adicionado ao banco de dados do sistema de tarifação, o mesmo deverá iniciar o processo de reconhecimento, adição do custo, inclusive markup, e alocação à respectiva entidade hierárquica no sistema.

Personalização de relatórios, cada evento gerador de custo dentro da solução deverá estar atrelada a uma entidade agrupadora e pronto para a geração de relatórios;

Uma vez criados os relatórios, deverá ser possível agendar o envio dos mesmos, podendo ser estabelecido um período de tempo. As saídas suportadas devem ser: arquivos em diversos formatos, e-mail ou diretamente às impressoras na rede;

Exportação de dados deverá permitir que em um período determinado pelo usuário os dados sejam disponibilizados;

Cada acesso a solução deverá ser realizado através de login e senha e ter diferentes privilégios à navegação;

Entre os privilégios ao acesso deve-se ter por localidades, por níveis hierárquicos pré-definidos, níveis de manipulação de dados, privilégios de configuração da solução, privilégios de configuração de relatórios;

A solução de tarifação deverá possuir uma ferramenta de análise de dados on-line que tenha como resultados alertas pró-ativos que possam ser distribuídos a usuários por e-mail ou mostrados na tela dos mesmos. Alguns alertas pró-ativos que devem ser gerados, são:

Uso excessivo de telefone;

Controle orçamentário (budget);

Devem ser gerados relatórios regulares e customizáveis, do tipo analítico e com gráficos anexos quando necessário, entre eles:

Relatório de conta resumida por DDR específico ou faixa de ramais;

Relatório detalhado por ramal, incluindo encaminhamentos realizados por este;

Sumários ou detalhados por órgão (Usuário/ Níveis Hierárquicos/ Centros de Custo/ Troncos/ Rotas internas);

Tráfego por Erlang por órgão;

Sumário por categorias por órgão;

Sumário por tipos de chamadas (saída, entrada, intra-rede saída / entrada, ramal-ramal, desviadas);

Diretório organizacional por Nível Hierárquico e/ou Centros de Custo;

Distribuição de uso por hora do dia;

Estatísticas de distribuição de chamadas (número discado) por entidade;

Ranking de números mais discados por duração, custos, quantidade e pulsos;

Ranking de usuários por duração, custos, quantidade e pulsos;

16.4.2.1. Históricos Mensais por Entidade

Os custos de chamadas (eventos) em VOIP deverão ser efetuados da forma tradicional ou por quantidade de bytes trafegados, informando o codec utilizado.

Possuir ferramenta para geração e envio de boletos de cobrança e/ou faturas por usuário, de acordo com o seu perfil, ou por divisão, como Diretoria, Secretaria, Superintendência, Órgão, consolidando na mesma seus devidos clientes com detalhamento de chamadas por ramal e pagamentos de impostos.

Permitir acesso dos 100.000 usuários via interface web para extração das informações de tarifação e bilhetagem, conforme perfil de acesso.

Os dados processados de toda a rede de voz deverão ser unificados em um único banco de dados, em padrão aberto ou comercial. Não serão aceitos sistemas com base

de dados proprietárias. Deverão ser criadas entidades de agrupamento chamadas usuário. Cada usuário deverá ser vinculado a uma hierarquia da rede.

Possibilitar a adição de custos fixos (ex. taxa de instalação) e/ou custos recorrentes (ex. aluguel de equipamento) por entidade usuário.

De acordo com privilégios, o usuário deverá poder visualizar uma janela de monitoração do andamento do sistema. Esta janela deverá alertar o usuário de eventuais falhas em algum processo da solução. Paralelamente, a solução de gerenciamento de falhas deverá enviar e-mail aos responsáveis por cada evento defeituoso para notificação. Caso a própria solução falhe, a interface de monitoramento deverá informar perda de comunicação e disparar localmente notificações urgentes aos responsáveis.

Possuir manual completo em inglês ou português.

16.4.3. Sistema (Software e Hardware) de Segurança para Acesso à Internet da Solução

Os dispositivos ofertados no sistema de segurança devem contemplar todas as especificações a seguir, podendo ser atendidos preferencialmente por um único equipamento (*appliance*) ou, alternativamente, por equipamentos separados.

16.4.4. Características de Firewall e VPN

Ser totalmente compatível com a solução e com ativos (gateways, softphone) de terceiros que implementem o padrão SIP (RFC 3261);

Operar em modo *stateful* e possibilitar a adição de, no mínimo, 1.000 (mil) regras (políticas de segurança);

Throughput mínimo de 300 (trezentos) Mbps para firewall;

Throughput mínimo de 100 (cem) Mbps para VPN, com criptografia AES e 3DES;

Número mínimo de conexões simultâneas: 50.000 (cinquenta mil);

Possuir no mínimo 6 (seis) interfaces de rede Ethernet 10/100/1000 (compatíveis com o padrão IEEE 802.3), com conectores RJ-45;

Fornecer bastidor tipo *rack*, possuindo porta frontal com chave e vidro temperado, compatível para instalação e acondicionamento da solução ofertada;

Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos") para a instalação dos equipamentos nos racks;

Dispor de fonte de alimentação com tensão de entrada de 120V a 240V AC (manual ou automática), e frequência de 60Hz;

Possuir led indicativo de on/off;

Possuir sistema operacional projetado e customizado especificamente para funções de firewall. Não serão aceitos sistemas de firewall que sejam executados sobre sistemas operacionais de mercado, como o *Novell NetWare*, e o *Microsoft Windows;*

Possuir uma interface serial (padrão DB-9 ou semelhante), para configuração e gerenciamento através de interface de linha de comando CLI (*Command Line Interface*);

Implementar o protocolo 802.1q, com a possibilidade de criação de diferentes VLANs, inclusive na mesma interface;

Prover mecanismo de conversão de endereços NAT (*Network Adress Translation*) e PAT (*Port Address Translation*), de forma a possibilitar que:

Mapeamento fixo 1-1 (Static NAT), permitindo com que servidores internos com endereços IP reservados sejam acessados externamente através de endereços IP válidos;

Redes ou ranges de endereços IP reservados acessem a Internet a partir de um ou mais endereços IP públicos (*Dynamic NAT*);

A conversão de endereços seja feita de acordo com critérios previamente estabelecidos, permitindo, por exemplo, que cada rede IP interna utilize um determinado range de endereços IP válidos de saída;

Os registros de eventos de NAT e PAT devem sempre conter as informações de portas e endereços internos e dos concedidos;

Fornecer criptografia e autenticação de pacotes IP, com chaves de criptografia de, no mínimo, 128 bits, de forma a possibilitar a criação de canais seguros (IPSEC VPNs) de forma a possibilitar:

Compatibilidade com o padrão IPSEC, de acordo com as RFCs 2401 a 2412, de modo a estabelecer canais de criptografia com outros produtos que também implementem tal padrão;

Permitir a criação de, no mínimo, 800 (oitocentos) túneis IP sobre IP (IPSEC *Tunnel*) simultâneos, de modo a possibilitar que as redes com endereços reservados possam se comunicar através da Internet;

Atribuir aos usuários de IPSEC VPN endereços IP reservados, tornando-os "virtualmente" parte da rede interna da solução;

Permitir o encapsulamento dos cabeçalhos IPSEC dentro de sessões UDP ou TCP, de forma que permita ao tráfego IPSEC passar por NAT ou quaisquer outros métodos de rede que necessitem alterar as propriedades do cabeçalho IP externo dos túneis IPSEC;

Possuir a capacidade de criação, manutenção e concentração de pelo menos 100 (cem) túneis SSL destinados a encapsular qualquer tráfego TCP/IP;

Possibilitar o controle do tráfego para os protocolos TCP, UDP e ICMP, baseado nos endereços de origem e destino e nos serviços utilizados na comunicação;

Possibilitar o controle do tráfego para os protocolos GRE, PIM e IGMP baseados nos endereços origem e destino da comunicação;

Possibilitar o controle do tráfego conforme o tipo (número) de protocolo IP;

Possibilitar o acompanhamento das conexões H323 e SIP "*inbound*" e "outbound", de forma a determinar as portas dinâmicas utilizadas nas transações de estabelecimento da chamada H323 ou SIP e automaticamente criar as regras ou mecanismos de segurança adequados, visando garantir a autenticidade da origem e destino envolvidos em cada chamada;

Possuir referências que limitam os números máximos de conexões de um mesmo cliente;

Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, Real Áudio, Real Vídeo, RTP, SRTP e SIP, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para tráfego *outbound* (de dentro para fora) quanto *inbound* (de fora para dentro);

Prover mecanismo contra ataques de falsificação de endereços (IP *Spoofing*) através da especificação da interface de rede pela qual uma comunicação deve se originar;

Prover proteção contra os ataques de negação de serviço SYN *Flood*, ICMP *Flood, Land*, *Tear Drop* e *Ping of Death*;

Para equipamentos apresentados separadamente, possibilitar integração com o agente de prevenção de intrusão (IPS) a ser adquirido, permitindo que estes agentes insiram regras temporárias no firewall, com duração pré-determinada, de forma automática;

Possibilitar a filtragem da linguagem *Javascript* e de *applets* Java e *Active-X* em páginas WWW, para o protocolo HTTP, permitir a utilização de LDAP e certificados X.509 (gravados em disco e/ou em *tokens* criptográficos/*smartcards*);

Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509, em conformidade com o padrão de PKI descrito na RFC 2459 (incluindo ICP Brasil), inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e/ou LDAP;

Implementar o protocolo SNMP (versão 2 ou posteriores);

Integração com MIBs que possam ser compiladas pelo HP *OpenView*;

Possuir manual de usuário completo em inglês ou português.

16.4.5. Características de Administração, Gerenciamento e Auditoria

Disponibilizar a configuração e gerenciamento dos firewalls por linha de comando CLI, acessível através de interface serial e das interfaces de rede (emulação de terminal Telnet ou SSH) ou por HTTP e HTTPS;

Possuir criptografia forte (chaves de criptografia iguais ou superiores a 128 bits) na comunicação através de SSH ou HTTPS;

Prover mecanismos de restrição de acesso remoto, através de filtros de endereços IP e usuário/senha;

Prover meios para criar, modificar, e excluir (além do padrão de fábrica) novos usuários e grupos administradores, pelo menos 02 (dois), com diferentes níveis de acesso (ex.: acesso total, leitura e escrita, somente leitura);

Permitir a conexão simultânea de vários usuários administradores, sendo pelo menos 01 (um) deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas;

Prover meios para criar, modificar, e excluir regras de acesso, através de, no mínimo:

Endereços IP de host(s);

Endereços IP de rede(s);

Protocolos e portas (IP, TCP e UDP);

Listas de acesso;

Dias e horários determinados.

Possuir criptografia forte (chaves de criptografia iguais ou superiores a 128 bits) na comunicação com o equipamento de gerenciamento;

Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas gráficas de alerta, e envio de Traps e mensagens SMTP;

Permitir a visualização, em *realtime* (tempo-real), de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall, além da remoção de qualquer uma destas sessões ou conexões;

Permitir a visualização de estatísticas do uso de CPU, memória ou utilização do equipamento;

Possibilitar o registro de toda ocorrência de mudanças nas configurações e demais aspectos importantes para auditoria do sistema;

Permitir o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;

Permitir o armazenamento e recuperação, através de protocolo criptografado, dos logs e eventos em máquinas remotas (Microsoft Windows NT/2000/2003, ou UNIX), e servidores de consolidação de logs, Syslog, ou Syslog-ng;

Possibilitar, a partir da console gráfica de gerenciamento e através de protocolo criptografado, a recuperação dos registros de log e eventos armazenados;

Possibilitar a aplicação de correções e atualizações para o sistema operacional e de firewall;

16.4.6. Características de Intrusion Prevenction System – IPS

Para equipamentos separados, apresentar as seguintes características:

Possuir sistema operacional projetado e customizado especificamente para funções de IPS. Não serão aceitos sistemas de IPS que sejam executados sobre sistemas operacionais de mercado, como o Novell NetWare, e o Microsoft Windows;

Possuir throughput total mínimo de 100 Mbps;

Possuir no mínimo 2 (duas) interfaces de rede 10/100 Mbps no padrão BaseTX, compatíveis com o padrão 802.3. Caso o *throughput* total seja maior do que 100 Mbps, as interfaces de rede deverão ser de 10/100/1000 Mbps;

Suporte a conexões full duplex;

Permitir a monitoração de VLANs, incluindo frames no padrão 802.1q;

Permitir a monitoração de redes MPLS;

Fornecer a capacidade de carregar todas as assinaturas em memória;

Capacidade de monitoração de segmentos de rede, posicionando-se tanto em modo promíscuo quanto em modo “in-line”, analisando cabeçalho (*header*) e área de

dados (*payload*) dos pacotes que trafegam em rede, detectando ataques ou tráfego não autorizado ou suspeito;

Capacidade de monitoração e detecção de intrusões nos protocolos SIP e H323;

Capacidade de monitoração de sessões de rede, atuando em modo *stateful inspection*, sendo capaz de detectar ataques ou tráfego não autorizado ou suspeito mesmo quando tal detecção não é possível via a monitoração de pacotes;

Possuir assinaturas de detecção baseadas em vulnerabilidades, permitindo a detecção de ataques desconhecidos e variantes de ataques sem a necessidade de assinaturas específicas;

Possuir análise e decodificação dos protocolos suportados nas 7 camadas OSI;

Realizar a detecção de anomalias e validação de protocolos;

Realizar análise de comportamento e heurística, capacidade de que novos ataques forem descobertos deverá possibilitar a criação de assinaturas associadas aos mesmos modos a prevenir tentativas de reincidência;

Possuir a capacidade de decodificação de múltiplos formatos de Unicode;

Possibilitar a fragmentação e defragmentação de IP e TCP *stream reassembly*;

Possuir a funcionalidade para detectar ataques em tempo real;

Possuir a capacidade de configurar ações, como TCP reset nas sessões TCP ou *Port Unreacheable* nas sessões UDP, de modo a evitar ataques baseados nestes protocolos;

Possuir a capacidade de monitorar o tráfego de redes TCP/IP, incluindo redes locais, conexões Internet e conexões discadas;

Possibilitar a analise de cada um dos pacotes que trafegam pela rede a que está conectado e também a relação de tais pacotes com os adjacentes a ele no fluxo de dados da rede. Identificar imediatamente, uma eventual violação da política de segurança, possibilitando o envio de alertas / alarmes para o software de controle;

Permitir o bloqueio de uma tentativa de invasão sem afetar os demais usuários conectados a rede;

Permitir a detecção e a prevenção das seguintes classes de ataques:

Ataques com nomes específicos, tais como PHF e Smurf;

Ataques genéricos (ataques nomeados com múltiplas variações), tais como Pacotes IP fragmentados e Teardrop;

Ataques como RTP *Session Hijacking* e Injeção de pacotes RTP não autenticados em comunicação existente;

Ataques ao Servidor de Comunicação Central e Gateways, *Denial of Service* (DoS), *Distribuited Denial of Service (DDoS*), *Scanning Attacks, Malformed Messages, Buffer Overflow*, FTP *exploits*, acesso não autorizado e *Probin Attacks*;

Possibilitar a atualização automática das "assinaturas" através de download seguro via Web. Para tanto, devem ser observadas as especificações da e-PING (www.eping.e.gov.br) para o componente "Transferência de arquivos de forma segura", ou seja, o uso do HTTPS (RFC 2818) ou do FTP (RFC 959 e RFC 2228);

Permitir a utilização de acesso via SSH para comunicação e configuração segura;

Realizar a verificação do TCP *Three Way Handshake*;

Permitir captura de log de sessão no formato padrão TCP *Dump*;

Oferecer respostas em tempo real para os ataques via rede, com possibilidade de término da sessão e reconfiguração de regras de acesso no processo firewall do mesmo dispositivo;

Permitir a verificação de decodificação de protocolos, scripts CGI, DNS, acesso remoto via BIND*, daemons,* serviços de diretórios (LDAP), chamados a procedimentos remotos (RPC);

Permitir a customização de respostas à intrusões, criação de conexões e modificação de ações de resposta;

Possuir ferramentas de configuração com interface gráfica;

Utilizar base de dados em tempo real para ajuda a resposta a incidentes ocorridos;

Gerar sumários de relatórios das atividades registradas;

Possibilitar o envio de e-mail e *traps* SNMP das informações da console de gerenciamento do produto;

Permitir o gerenciamento de incidentes através de relatórios técnicos e gerenciais pré-definidos, com detalhamento das informações coletadas;

Permitir a criação de relatórios técnicos e gerenciais personalizados, em formas textuais e gráficas;

Fornecer documentação detalhada para possibilitar a configuração;

Permitir configuração remota, a partir da console de gerenciamento, fornecendo a capacidade de *encriptar* esta comunicação, isto é, o evento enviado a console de gerenciamento e as configurações recebidas deverão ser encriptadas;

Possuir a capacidade de resposta em tempo real para tratamento de ataque direcionado ao próprio equipamento;

Possuir a capacidade de enviar alertas vias SNMP (traps SNMP para o sistema de gerenciamento da rede);

Possuir a capacidade de enviar alerta via SMTP (envio de e-mails);

Ter uma base de assinaturas que permita atualizações automáticas e periódicas;

Implementar a modificação de assinaturas, isto é, permitir a edição de assinaturas existentes na base de dados, ajustando-se ao perfil de tráfego de rede MAN;

Possibilitar a criação de assinaturas, isto é, permitir que se possam criar novas assinaturas e anexá-las a base de dados existente;

Fornecer a gravação de todos os eventos em Logs, sem intervenção de agente não integrado ao hardware e/ou de desenvolvimento não efetuado pelo próprio fabricante / desenvolvedor do hardware;

Fornecer a geração de relatórios customizados, por horário, por evento, por endereço IP de origem ou destino, por porta e demais campos registrados na base de eventos;

Fornecer a capacidade de encriptar toda a comunicação com a console, isto é, o evento enviado à console de gerenciamento e as configurações recebidas deverão ser encriptadas;

Possuir uma base de dados com no mínimo 300 (trezentas) vulnerabilidades para detecção;

Fornecer configuração do dispositivo através de linha de comando (CLI), WEB ou console de Gerencia;

Capacidade de prevenção de intrusos e ataques efetuados no tronco de rede que esteja sendo monitorado e/ou analisado;

(Realizar a detecção de anomalias e validação de protocolos;

Fornecer a função de descartes dos pacotes que provocaram o evento;

Bloquear ataques de acesso não autorizado;

Bloquear vírus auto replicantes;

Isolar código malicioso que está contido dentro de código aparentemente inofensivo;

Bloquear tentativas de invasão, desde que a assinatura/protocolo permita efetuar alguma modalidade de bloqueio;

Permitir customização de respostas a intrusões, mascaramento de tráfego, criação de conexões e modificação de ações de resposta;

Caso seja um equipamento separado do firewall, possuir funcionalidade de *Bypass*, garantindo que em caso de falha ou indisponibilidade do equipamento (mesmo desligado), os serviços do segmento protegidos continuem disponíveis.

16.5. Gateways de VOZ sobre IP

16.5.1. Características Comuns a todas as Classes

Para equipamento único, o mesmo deve ser do tipo appliance e possuir processadores, discos rígidos, interfaces de rede tipo Ethernet 10/100 Mbps, ventiladores e fontes de alimentação operando em 110 ou 220 VAC de entrada, 60 HZ, fase/neutro/terra. Todos estes componentes devem ser duplicados e redundantes entre si

(exceto em gateways das Classes I e VII), operar em modo Fail Over, hot-swappable e capazes de suportar a capacidade máxima de processamento do equipamento ofertado.

Não serão aceitos PC's ou equipamentos baseados em PC's;

Para equipamentos separados, cada um deve ser do tipo appliance e possuir, no mínimo, 2 (duas) interfaces de rede tipo Ethernet 10/100 Mbps, fonte de alimentação operando em 110 ou 220 VAC de entrada, 60 HZ, fase/neutro/terra. Não serão aceitos PC's ou equipamentos baseados em PC's;

Possuir alimentação elétrica alternativa (no-breaks) com:

Entradas de alimentação redundantes operando em 110 e 220 VAC automático, 60 HZ, capazes de suportar a capacidade pedida, incluindo as expansões, de cartões/módulos dos equipamentos ofertados;

Garantia a continuidade do serviço provido pelo gateway por um período mínimo de 4 (quatro) horas, em caso de falha de energia elétrica (em plena carga);

Sinalização visual para modo de fornecimento de energia pela rede elétrica ou bateria;

Sinalização indicativa de fim da carga da bateria;

Proteção contra descarga total das baterias com sinalização antes do desligamento;

Gerar alarmes via SNMP e possibilitar o envio dos mesmos a destinatário(s) de Correio Eletrônico (e-mail);

Possuir interfaces para conexões E1, FXS e/ou FXO de entrada e de saída, de acordo com a sua classe, bem como cabos compatíveis com o PABX a ser conectado;

Fornecer bastidor tipo rack, possuindo porta frontal com chave e vidro temperado, compatível para instalação e acondicionamento para cada equipamento ofertado;

Atender aos seguintes padrões:

IP (*Internet Protocol* - RFC 0791);

TCP (*Transmission Control Protocol* - RFC 0793);

UDP (*User Datagram Protocol* - RFC 0768);

DNS (*Domain Name System* - RFC 1034);

FTP (*File Transfer Protocol* - RFC 0959) ou TFTP (Trivial File Transfer Protocol - RFC 1350);

ICMP (Internet Control Message Protocol - RFC 0792);

NTP (*Network Time Protocol* - RFC 1305);

SNMP v2 (*Simple Network Management Protocol* - RFC 1905) ou superior;

SIP (Session Initiation Protocol - RFC 3261);

SDP (Session Description Protocol - RFC 2327);

RTP (*Real-Time Transport Protocol* - RFCs 1889 e 1890);

SRTP (*Secure Real-time Transport Protocol* - RFC 3711);

Implementar os protocolos de sinalização ISDN/RDSI: QSIG, CAS e R2BR; e IP: SIP.

Deve implementar os protocolos de Fax T.30 ou T.38, *Real-Time* Fax sobre IP;

Implementar os padrões de áudio ITU G.711, G.723, G.729, devendo o equipamento ofertado possuir capacidade de processamento da capacidade máxima de tráfego em qualquer um dos padrões citados, sem perda ou atraso na comunicação;

Os equipamentos devem ser compatíveis as diversas categorias de PABXs (PABX Digital, Híbrido e IP) de diversos fabricantes a serem interligados, sem perda de qualidade ou facilidades;

O equipamento deve se comunicar com outros gateways e com o Servidor de Comunicação Central utilizando padrão aberto SIP. Deste modo, o equipamento deverá ser capaz de se registrar no Sistema Central e estabelecer chamadas em SIP, utilizando os protocolos RTP e SRTP para transmissão de voz.

Inclusive, o equipamento deve ser capaz de implementar o protocolo SRTP em todos seus canais SIP simultaneamente;

O equipamento deve ser compatível com o Sistema Central redundante, comutando automaticamente o seu registro e sinalização para o outro equipamento do Sistema Central, caso o primeiro se torne inacessível;

Implementar os processamentos de voz VAD (Voice Activity Detection), G.165 ou G.168 (cancelamento de eco), CNG, TIA-464B DTMF;

Permitir atualizações via FTP ou TFTP;

Implementar redirecionamento de tráfego RTP e SRTP, permitindo que o tráfego de voz-sobre-IP vá diretamente de um terminal ao outro sem passar pelo Servidor de Comunicação;

Deverá ser possível o equipamento realizar automaticamente o escoamento de todo o tráfego para a interface com a RPT, caso seja detectado indisponibilidade da rede MAN;

Implementar Qualidade de Serviço (QoS), utilizando no mínimo DiffServ (CoS) e IP Precedence (ToS);

O sistema deve conter buffers dinâmicos para controle de jitter;

Possuir MIBs para o envio, via SNMP, de todos os dados necessários para satisfazer as características exigidas no Sistema de Gerenciamento, Monitoramento e Manutenção;

Possuir manual completo em inglês ou português.

16.5.1.1. Especificidades de cada Classe

Classe I – Possuir capacidade de processamento e interfaces para 2 (duas) conexões E1, suportando expansão em modo hot-swappable para pelo menos 4 (quatro). A conexão IP total com o Switch da MAN deve ser de 20 (vinte) canais SIP, suportando expansão para pelo menos 30 (trinta) canais. Caso o equipamento não suporte expansão, o mesmo deverá ser apresentado com sua capacidade máxima (4 E1 e 30 canais SIP).

Classe II – Possuir capacidade de processamento e interfaces para 4 (quatro) conexões E1, suportando expansão em modo hot-swappable para pelo menos 6 (seis). A solução deverá ser apresentada: ou em equipamento único com redundância interna,

com o hardware estando de acordo com o Item 2.2.1, Letra “a)”, ou, alternativamente, em dois equipamentos redundantes entre si e apresentando as interfaces de acordo com a Tabela 2, além de possuir hardware de acordo com o Item 2.2.1, Letra “b)”. A conexão IP total com o Switch da MAN deve ser de 60 (sessenta) canais SIP, suportando expansão para pelo menos 90 (noventa) canais. Caso o equipamento não suporte expansão, o mesmo deverá ser apresentado com sua capacidade máxima (6 E1 e 90 canais SIP).

Classe III – Possuir capacidade de processamento e interfaces para 6 (seis) conexões E1, suportando expansão em modo hot-swappable para pelo menos 8 (seis). A solução deverá ser apresentada: ou em equipamento único com redundância interna, com o hardware estando de acordo com o Item 2.2.1, Letra “a)”, ou, alternativamente, em dois equipamentos redundantes entre si e apresentando as interfaces de acordo com a Tabela 1, além de possuir hardware de acordo com o Item 2.2.1, Letra “b)”. A conexão IP total com o Switch da MAN deve ser de 80 (oitenta) canais SIP, suportando expansão para pelo menos 120 (cento e vinte) canais. Caso o equipamento não suporte expansão, o mesmo deverá ser apresentado com sua capacidade máxima (8 E1 e 120 canais SIP).

Classe IV – Possuir capacidade de processamento e interfaces para 8 (oito) conexões E1, suportando expansão em modo *hot-swappable* para pelo menos 12 (doze). A solução deverá ser apresentada: ou em equipamento único com redundância interna, com o hardware estando de acordo com o Item 2.2.1, Letra “a)”, ou, alternativamente, em dois equipamentos redundantes entre si e apresentando as interfaces de acordo com a Tabela 2, além de possuir hardware de acordo com o Item 2.2.1, Letra “b)”. A conexão IP total com o Switch da MAN deve ser de 120 (cento e vinte) canais SIP, suportando expansão para pelo menos 180 (cento e oitenta) canais. Caso o equipamento não suporte expansão, o mesmo deverá ser apresentado com sua capacidade máxima (12 E1 e 180 canais SIP).

Classe V – Possuir capacidade de processamento e interfaces para 12 (doze) conexões E1, suportando expansão em modo *hot-swappable* para pelo menos 16 (dezesseis). A solução deve ser apresentada ou em equipamento único com redundância interna, com o hardware estando de acordo com o Item 2.2.1, Letra “a)”, ou,

alternativamente, em dois equipamentos redundantes entre si e apresentando as interfaces de acordo com a Tabela 1, além de possuir hardware de acordo com o Item 2.2.1, Letra "b)". A conexão IP total com o Switch da MAN deve ser de 160 (cento e sessenta) canais SIP, suportando expansão para pelo menos 240 (duzentos e quarenta) canais.

Caso o equipamento não suporte expansão, o mesmo deverá ser apresentado com sua capacidade máxima (16 E1 e 240 canais SIP).

Tabela 2 – Distribuição de interfaces em equipamentos para cada Classe, Siemens do Brasil, (2009)

Classe	**Qtde. de interfaces para o equipamento único**	**Qtde. de interfaces para cada equipamento separado**	
I	2 E1	-	
II	4 E1	2 E1	2 E1
III	6 E1	3 E1	3 E1
IV	8 E1	4 E1	4 E1
V	12 E1	6 E1	6 E1

16.6. Valor Estimado de um Sistema VOIP à ser Implantado

Em cumprimento ao disposto no inciso III do Art. 9º do Decreto nº 3.931/2001, divulga-se o preço unitário máximo que a Administração se dispõe a pagar pelos bens. São apresentados os valores mediante as necessidades dos órgãos, valores aproximados.

16.6.1. Penalidades

A recusa injustificada da empresa com proposta classificada na licitação e indicada para registro dos respectivos preços na cláusula DISPOSIÇÕES GERAIS ensejará a aplicação das penalidades enunciadas no art. 87 da Lei Federal nº 8.666/93,

bem aquelas introduzidas pela Lei nº 10.520/2002 e Decreto nº 3.555/2000, a critério da Administração.

A recusa injustificada, da detentora desta Ata, em assinar o contrato dentro do prazo de 5 (cinco) dias úteis, contados a partir do recebimento da data de sua convocação, por escrito, implicará na aplicação da multa de 10% (dez por cento) do valor da mesma.

Pela inexecução total ou parcial das obrigações assumidas nesta Ata de Registro de Preços, a Administração poderá aplicar, à detentora da Ata, as seguintes penalidades, sem prejuízo das demais sanções legalmente estabelecidas:

16.6.1.1. As multas serão aplicadas da seguinte forma

a) multa compensatória no percentual de 10% (dez por cento), calculada sobre o valor total estimado do contrato, pela recusa em assiná-lo, apresentar o comprovante da prestação da garantia de funcionamento ou retirar a Nota de Empenho, no prazo máximo de 05 (cinco) dias úteis, após regularmente convocada, por escrito, sem prejuízo da aplicação de outras sanções previstas no subitem 30.1 deste Edital;

b) multa de mora no percentual correspondente a 0,5% (meio por cento), calculada sobre o valor total do contrato, por dia de inadimplência, até o limite de 02 (dois) dias, na prestação de serviços, caracterizando inexecução parcial.

c) multa compensatória no percentual de 10% (dez por cento), calculada sobre o valor total do contrato, pela inadimplência além do prazo acima o que ensejar a rescisão do contrato.

As importâncias relativas a multas serão descontadas dos pagamentos a serem efetuados à detentora da Ata, podendo, entretanto, conforme o caso, processar-se a cobrança judicialmente.

As penalidades serão aplicadas sem prejuízo das demais sanções cabíveis, sejam estas administrativas ou penais, previstas na Lei nº 10.520/2002 e Decreto nº 3.555/2000.

16.6.1.2. Autorização para Aquisição

As aquisições do objeto, serão autorizadas, caso a caso, pelo Subsecretário de Planejamento, Orçamento e Administração do MP, e no caso dos órgãos usuários pela respectiva autoridade responsável.

A emissão das ordens de fornecimento, sua retificação ou cancelamento, total ou parcial deverão ser igualmente autorizados pelo órgão requisitante.

16.7. Aquisição de Equipamento para solução de Voz

16.7.1. Objetivo

Aquisição de Servidor Central de Comunicação e Gateways de Voz sobre IP para compor solução de integração do sistema de telefonia de órgãos e entidades da Administração Pública Federal, compreendendo fornecimento, instalação, ativação, transferência de tecnologia e garantia de funcionamento, segundo .

16.7.1.2. Descrição da Solução

A integração dos sistemas de telefonia local se dará através de uma infraestrutura de rede ótica que interliga diversos órgãos e entidades governamentais localizados em Brasília doravante denominada. Rede Metropolitana (MAN). A MAN trabalha no padrão *Gigabit Ethernet* (*Metro Ethernet*) e possuí um switch de acesso em cada órgão interligado, no qual é efetuada a troca de tráfego com a rede local do órgão.

A solução, seguindo as melhores práticas e tendências de mercado, deverá ser implementada no padrão SIP, conforme RFC 3261, incluindo a comunicação entre os Gateways e também com o Servidor de Comunicação Central. Assim, além de outras funções, este último atuará como um SIP Proxy Server em modo *stateful* e como SIP Registrar Server, intermediando chamadas entre os *Gateways* e outros ativos SIP (a exemplo do software denominado *Asterisk).* O Servidor de Comunicação Central deverá ser capaz de receber e manter registros de terminais SIP, Gateways e SIP *Proxy Servers* de órgãos que possuam ou venham a possuir solução de VOIP local baseada no padrão SIP.

Além da comunicação entre os Sistemas de Telefonia Local dos órgãos interligados à MAN, a solução deverá permitir ligações com a Internet para comunicações remotas, através de um *softphone*, por exemplo.

A comunicação de voz, incluindo o acesso à Internet, deverá ser seguro, através do Sistema de Segurança composto de firewall, IPS e concentrador de VPN. Dentro da MAN, será utilizado o protocolo SRTP para a criptografia e autenticação entre os gateways.

A solução será implantada em 2 (duas) etapas. A primeira consiste em prover o serviço de voz compreendendo apenas o tráfego interórgãos, também chamada de voz corporativa. Já a segunda deverá tratar todo tráfego originado nos órgãos. A proponente deverá fornecer a solução configurada para primeira etapa, devendo efetuar as configurações necessárias para segunda etapa quando for solicitado. Para tanto, os equipamentos a serem fornecidos devem estar preparados para as duas etapas, sem que seja necessária qualquer complementação de hardware.

16.7.1.2.1. Primeira Etapa de Roteamento

Em um órgão pertencente à MAN, as ligações telefônicas destinadas a outros órgãos pertencentes à própria rede serão roteadas internamente pela infraestrutura da MAN. As demais ligações serão direcionadas para Rede Pública de Telefonia (RPT).

Cada órgão terá sua Central Telefônica (PABX) interligada à MAN via gateway de Voz sobre IP (VOIP). Este equipamento também deverá ser capaz de direcionar as chamadas para dentro da MAN ou para RPT, conforme o caso, devendo possuir as interfaces necessárias para tanto. Cada gateway estará conectado a uma porta do switch de acesso da MAN, que fará parte de uma Rede Virtual (VLAN) interórgãos dedicada exclusivamente para tráfego de Voz, mapeando-se nestas tão somente as portas dos switchs da MAN.

Todas as ligações originadas pelo órgão serão encaminhadas ao gateway, que fará o devido direcionamento das mesmas. Nesta etapa, o órgão manterá suas conexões com a RPT, sendo que as conexões de entrada se ligarão ao PABX e, as de saída, ao gateway.

O tráfego interórgãos será gerenciado, monitorado e bilhetado por um Servidor de Comunicação Central, que deverá ter capacidade e disponibilidade para tanto.

A figura 13, mostra a topologia , o cenário de como funciona o tráfego.

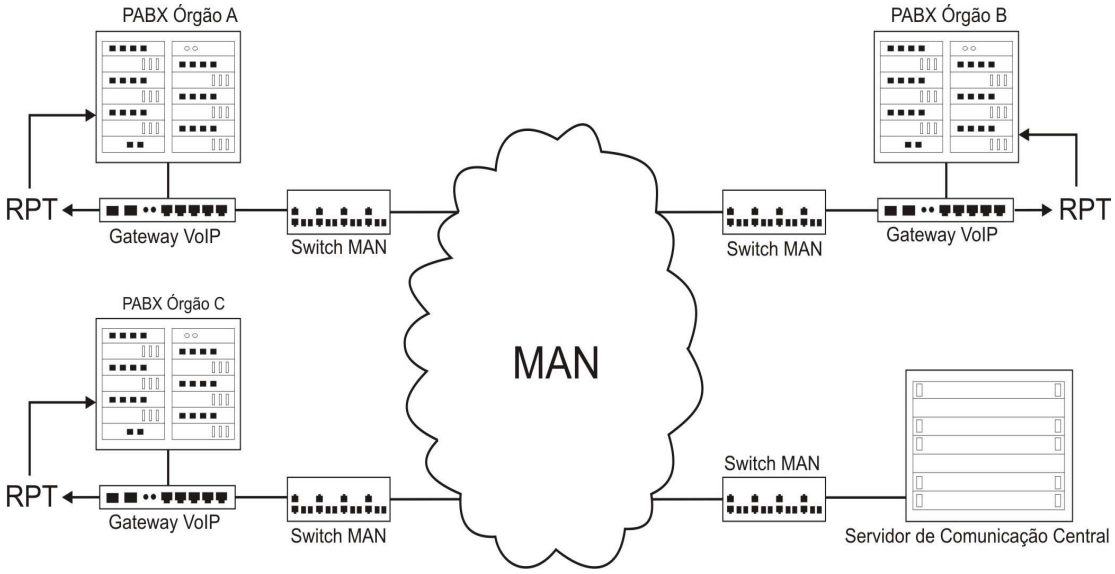

Figura 13 – Topologia da Solução de Integração de Voz para Primeira Etapa, Siemens, (2009)

16.7.1.2.2. Segunda Etapa de Roteamento

Esta etapa é uma evolução da primeira, na qual todo o tráfego de saída de cada órgão será entregue pelo gateway diretamente à MAN. Assim, os gateways não terão mais conexões de saída com a RPT.

O Servidor de Comunicação Central deverá ser capaz de analisar, processar, redirecionar e bilhetar todo o tráfego de saída dos órgãos conectados à MAN, roteando internamente pela MAN as ligações pertencentes à própria MAN e direcionando as demais para a RPT, que estará conectada ao mesmo.

O Servidor de Comunicação Central deve ser dimensionado de forma que as chamadas em SIP (IP) estabeleçam direta conexão com a RPT, dispensando assim interfaces E1. Esta característica está considerada na especificação do Servidor.

Nesta etapa, os órgãos continuarão a manter sua conexão de entrada com a RPT, para receberem todas as chamadas externas (ligações que não sejam dos outros órgãos pertencentes à MAN).

O esquema da figura 14, ilustra a etapa de Roteamento

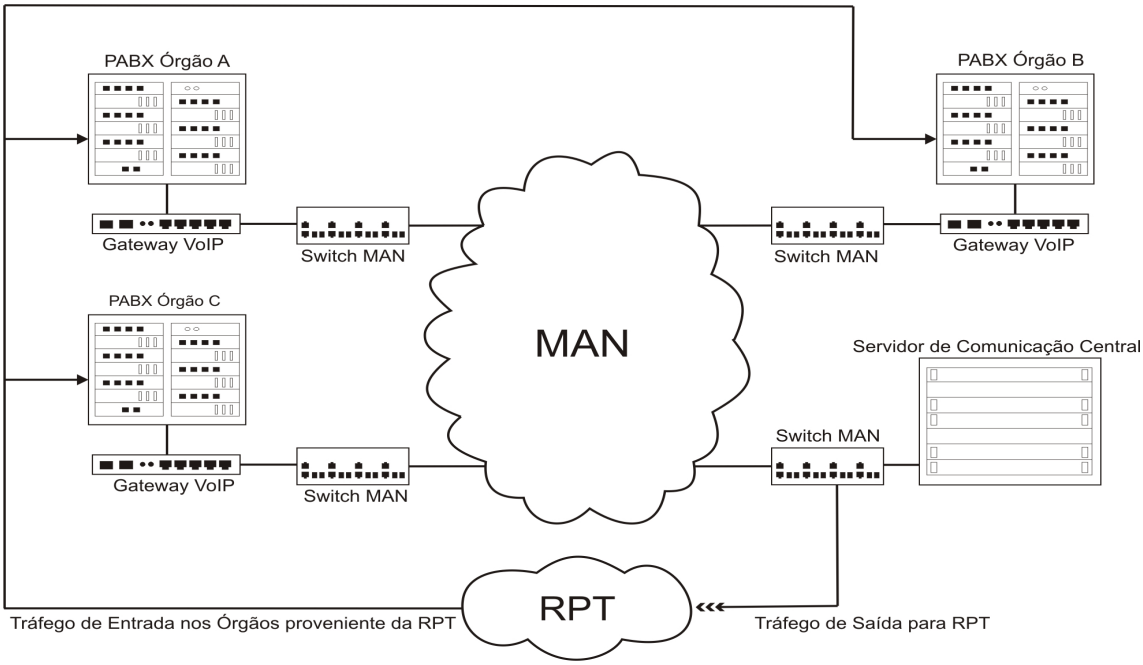

Figura 14 – Topologia da Solução de Integração de Voz. Fonte: Siemens, (2009)

16.7.2. Proposta de Preço do Sistema VOIP à ser Implantado

Segundo Siemens, (2010) a proposta apresentada de preços são sugeridos conforme necessidade das empresa, portanto para esse exemplo o pagamento será realizado em uma única parcela, até o 5º (quinto) dia útil após a entrega dos equipamentos bem como após o término da capacitação da equipe de técnicos da Administração Pública, mediante a apresentação da Nota Fiscal acompanhada do Termo de Aceite.

A proposta, em que será apresentado o preço global da solução, compreenderá a descrição dos equipamentos ofertados e seus preços unitários e totais, e deverá ser compatível com todos os itens deste Termo de Referência e seu Anexo, bem como atender às exigências da legislação vigente.

Os equipamentos em questão serão tombados como Material Permanente, sendo que a proponente deverá levar isto em consideração em sua proposta, para fins de tributação.

A proposta deverá discriminar, para cada equipamento cotado, os seus componentes e respectivos valores.

A proposta deverá conter o detalhamento da solução de forma clara, incluindo um diagrama topológico completo, descrevendo detalhadamente as características técnicas dos equipamentos ofertados, incluindo especificação de marca, modelo, procedência e outros elementos que de forma inequívoca identifiquem e constatem as configurações cotadas, comprovando-os através de certificados, manuais técnicos, folders e demais literaturas editadas pelo fabricante.

A omissão da resposta de quaisquer dos quesitos de avaliação, tais como folders, informações técnicas ou outra documentação que comprove a veracidade das informações, implicará na desclassificação da proposta.

Para cada equipamento cotado na proposta, deverá ser entregue 1 (um) jogo completo de manuais do respectivo fabricante.

A proponente deverá garantir em sua proposta, para avaliação e concordância, documentação contendo os detalhes técnicos que comprovem o atendimento das especificações e funcionalidades dos equipamentos (e softwares incluídos).

Na proposta deverão ser apresentadas, ainda, quaisquer outras informações afins, que a proponente julgar necessárias ou convenientes.

16.8. Habilitação Técnica

A proponente deverá apresentar Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, declarando ter a proponente desenvolvido e implantado uma solução de telefonia composta por Gateways que se comuniquem entre si e com um Servidor Central de Comunicação, sendo os equipamentos fornecidos compatíveis e pertinentes a solução de segurança em serviço VOIP.

A proponente deverá apresentar documento relacionando sua Assistência Técnica, com endereço, telefone, fax, e-mail e responsável para contato. A Assistência

Técnica deverá possuir, pelo menos, 2 (dois) técnicos lotados na localidade do sistema implantado e treinados pela(s) fabricante(s) do Servidor Central de Comunicação e dos Gateways cotados, possuindo diploma ou certificado emitido pela(s) mesma(s). A comprovação será feita por meio de cópia da carteira de trabalho, ficha funcional, diplomas e certificados.

A proponente deverá comprovar dispor de central de atendimento para abertura de chamados na modalidade 24 X 07 (horário integral).

A proponente deverá fornecer declaração do fabricante do Sistema Central garantindo interoperabilidade no padrão SIP com o software livre *Asterisk* (versão 1.2.7.1, datada de 13/04/2006 ou outra superior) e pelo menos um *softphone*, também em software livre. Além disso, a declaração deverá conter garantia de interoperabilidade com telefones IPs e gateways E1-SIP de pelo menos 3 (três) fabricantes para cada. A declaração em questão não implica necessariamente no suporte aos equipamentos e softwares mencionados acima.

A proponente deverá apresentar o(s) Certificado(s) de Homologação emitido pela ANATEL, referentes aos gateways que se conectarão à RPT, conforme determina a Resolução Nº 242 da ANATEL, de 30 de novembro de 2000.

16.8.1. Entrega, Instalação e Avaliação

Os equipamentos especificados neste Termo de Referência deverão ser entregues pela proponente em perfeitas condições de operação na Divisão de Patrimônio do Ministério, no prazo máximo de 45 (quarenta e cinco) dias corridos e devendo a entrega ser informada com, no mínimo, 5 (cinco) dias corridos de antecedência.

No ato da entrega, a equipe de recepção composta de técnicos do Ministério e com o apoio de técnicos da proponente efetuará as inspeções e testes necessários para verificação da conformidade de cada equipamento.

Finda a etapa de recepção, a proponente providenciará a configuração e instalação final de cada equipamento em seus locais definitivos, a serem informados por ocasião da entrega, com acompanhamento de técnicos deste Ministério e dos órgãos e

entidades em que os equipamentos serão instalados, no prazo máximo de 10 (dez) dias úteis.

A instalação dos equipamentos será física e lógica, compreendendo todas as conexões e configurações necessárias com o PABX e o Switch de Acesso da MAN, em cada órgão ou entidade a que se destinarem, sendo que a solução de integração de voz referente à primeira etapa deverá estar totalmente operacional ao final da instalação.

Também deverão ser efetuados, em conjunto com técnicos dos órgãos e entidades, ajustes que eventualmente sejam necessários nos PABX. Além disso, a proponente deverá apoiar as configurações na MAN necessárias ao perfeito funcionamento da solução, repassando toda e qualquer informação técnica pertinente à adequação da Rede Metropolitana para receber e suportar a Solução de Voz.

A proponente entregará, ao final, toda a documentação de instalação da solução, incluindo os detalhes de configuração de cada equipamento e diagramas topológicos. A documentação deve prover um nível de informação suficiente para que um técnico possa entender e refazer as configurações do sistema.

Os testes de aceitação, que serão realizados ao término dos trabalhos de instalação e configuração, compreenderão a realização em conjunto com a equipe do Ministério de atividades de operação e gerência do sistema. Estes testes têm como objetivo a avaliação da solução entregue, verificando a conformidade com as especificações técnicas deste Edital, bem como a análise do perfeito funcionamento da solução de Integração de Voz e dos equipamentos que a compõem, estando de acordo com a proposta neste documento. Somente com a aprovação destes testes que será lavrado o Termo de Aceite.

16.9. Garantia de Funcionamento e Níveis de Serviço

A proponente deverá garantir a completa interoperabilidade e compatibilidade dos componentes de hardware e software utilizados na solução, particularmente em consonância com as premissas estabelecidas no documento de referência da arquitetura de Padrões de Interoperabilidade de Governo Eletrônico (e-PING), disponível no endereço eletrônico http://www.eping.e.gov.br.

A proponente deverá garantir a funcionalidade “fim-a-fim” da solução, a plena interconexão em SIP entre os Gateways e com o Servidor Central de Comunicação, assim como a interoperabilidade com os PABXs a serem interligados na MAN, tendo para tanto efetuado os testes necessários, garantindo a recepção, tratamento e encaminhamento do tráfego em SIP originado no Gateway. Exclui-se da garantia apenas a conectividade da MAN. Define-se conectividade como o recebimento e a entrega do tráfego na camada de enlace do modelo OSI pelas portas Gigabit Ethernet dos switches da MAN.

Além disso, a proponente deverá garantir que a solução ofertada possua comunicação irrestrita e completa, no padrão SIP, SDP, RTP e SRTP, com Gateways de outros fabricantes que possuam implementado tais padrões, incluindo o software livre *Asterisk.*

A proponente deverá garantir pleno funcionamento dos equipamentos, responsabilizando-se por qualquer componente adicional que for identificado após a contratação, seja por motivos de interoperabilidade, compatibilidade ou quaisquer outros motivos que impeçam o funcionamento efetivo da solução de integração de voz.

A proponente efetuará a operação assistida do sistema durante 1 (um) ano, contado a partir emissão do Termo de Aceite, período no qual manterá 2 (dois) técnicos residentes junto ao Servidor de Comunicação Central, os quais devem ser certificados pelo fabricante do mesmo. A operação assistida não se confunde com a Assistência Técnica, que deverá ser prestada em horário integral. O serviço de operação assistida, por sua vez, será prestado durante o período de 08 (oito) horas diárias, com intervalo escalonado de 02 (duas)} horas para almoço, de segunda a sexta-feira, sendo o mesmo o horário dos técnicos residentes;

Durante o período de operação assistida, a proponente, em conjunto com a equipe de técnicos indicada pelo Ministério, deverá executar todas as configurações e atividades necessárias à operação do sistema. Neste sentido, a responsabilidade pela operação será da proponente, que também estará supervisionando e orientando a equipe indicada, de modo que, ao final do tempo de operação assistida, esta equipe esteja capacitada a assumir a gestão do sistema.

É responsabilidade da proponente a correção das falhas decorrentes de erros durante as atividades de instalação, sejam operacionais ou por problemas de mau funcionamento dos equipamentos, responsabilizando-se por todos os custos envolvidos na correção dos desvios, sejam de interoperabilidade, incompatibilidade ou quaisquer outras falhas que impeçam a instalação ou o perfeito funcionamento dos serviços de telefonia.

Eventuais despesas de custeio com deslocamento de técnicos da proponente ao local de instalação, bem como todas as despesas de transporte, diárias, seguro ou quaisquer outros custos envolvidos ficam a cargo exclusivo da proponente.

O prazo para garantia de funcionamento e suporte técnico da solução, inclusive no local de instalação dos equipamentos, deverá ser, no mínimo, de 24 (vinte e quatro) meses, contados a partir da data de emissão do Termo de Aceite.

A proponente deverá fornecer garantia do fabricante para os equipamentos cotados por um período mínimo de 24 (vinte e quatro) meses, contados a partir da data de emissão do Termo de Aceite.

A manutenção corretiva será realizada em período integral, 7 (sete) dias por semana e 24 (vinte e quatro) horas por dia, após solicitação do Ministério, ou de quem este delegar, por meio de telefonemas, notificação via fax ou mensagens eletrônicas;

Os chamados serão registrados e deverão estar disponíveis para acompanhamento pela equipe do Ministério, ou de quem este delegar, contendo data e hora da chamada, o problema ocorrido, a solução, data e hora de conclusão.

16.10. Obrigações da Contratante

Compete à CONTRATANTE:

a) Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento dos equipamentos;

b) Efetuar o pagamento à contratada até o 5º (quinto) dia útil após apresentação da Nota Fiscal e o Termo de Aceite; e

c) Observar e fazer cumprir fielmente o que estabelece o Termo de Referência (Siemens, 2010) , em especial os itens 6, 7 e 8 (seis, sete e oito), que tratam da entrega, instalação, avaliação, capacitação, garantia de funcionamento e níveis de serviço.

PARÁGRAFO ÚNICO

No preço proposto estão incluídos todos os custos diretos e indiretos, inclusive o serviço de assistência técnica durante o período de garantia oferecido pela CONTRATADA, frete, seguro, material, tributos e/ou impostos, taxas, bem como quaisquer outras despesas incidentes na execução do Contrato.

17. Melhores Práticas de Segurança em Serviço VOIP

A figura 15, demonstra abaixo o funcionamento de uma VOIP.

Figura 15 - Estrutura VOIP, Fonte: Revista RTI, 2010

Portanto, segundo Lawrence, (2009) e a revista RTI, (2010), sugere-se citar algumas das melhores práticas para garantir a segurança do Serviço VOIP:

1. Escolher com cuidado os protocolos do VOIP. Há prós e contras para vários protocolos e fornecedores de equipamento do VOIP, que serão mencionados no item de vantagens e desvantagem de VOIP. Certifique-se de selecionar equipamentos que

satisfaçam suas necessidades, e não o contrário. Mudar seus requisitos para dar suporte ao equipamento de um fornecedor específico é um péssimo hábito.

2. Desligar os protocolos desnecessários. Há vulnerabilidades suficientes que podem ser exploradas nos protocolos utilizados, serão mencionados também no item de vantagens e desvantagens. Não há necessidade de aumentar a "janela de oportunidade" dos hackers ao habilitar protocolos e serviços desnecessários e não utilizados. Isso deve ser seguido para os protocolos de VOIP, bem como para outros serviços fornecidos pelo equipamento de VOIP.

3. Qualquer elemento da infraestrutura de VOIP, acessível na rede, como qualquer outro computador, pode ser atacado. Mesmo que se pareçam com telefones e terminais, elementos de VOIP são componentes de software rodando em hardware. Certifique-se de que seja possível fazer a gestão do sistema operacional por trás desses componentes. Devido a considerações quanto ao ciclo de vida do desenvolvimento, alguns programas de gestão de VOIP são baseados em versões mais antigas de sistemas operacionais vulneráveis. Certifique-se de que também seja possível proteger esses elementos.

4. A estratégia de dividir para conquistar funciona bem em redes de VOIP. É altamente recomendado separar a infraestrutura de VOIP de outras infraestruturas, utilizando separadores físicos ou lógicos.

5. Autenticar operações remotas. Terminais de VOIP podem ser atualizados e que façam gestão remotamente. Certifique-se de utilizar somente pessoal autorizado em localizações autorizadas (com base nos endereços de IP e nomes de usuário únicos). Evite que um usuário remoto ataque seus serviços

6. Separar os servidores de VOIP da rede interna.Vários dispositivos de segurança não conseguem entender completamente os comandos de sinalização de VOIP. Consequentemente, eles podem abrir portas de comunicação dinâmicas, deixando a rede vulnerável a ataques de *bounce*. Isso pode permitir que um atacante penetre em elementos críticos aos negócios da empresa na LAN interna.

7. Certificar que o sistema de segurança VOIP possa rastrear as portas de comunicação. É ainda mais importante que os sistemas de segurança sejam capazes de entender a cadeia de operações adequada e fazer com que ela seja seguida. Caso

contrário, até mesmo um ataque de DoS simples, mas eficaz, pode desconectar os usuários, forjando mensagens de desconexão. Um sistema de segurança deve poder evitar esse tipo de ataque.

8. Utilizar NAT (Network Address Translation). Mesmo que em alguns casos isso apresente certos problemas para VOIP. NAT converte endereços de IP internos em endereços de IP únicos e globais para roteamento na Internet. O benefício adicional de esconder a rede é inestimável. Uma solução de segurança deve permitir que você habilite NAT na rede interna e que os usuários de fora da rede encontrem usuários com endereços de IP dinâmicos e não roteáveis.

9. Utilize um sistema de segurança que efetue verificações de segurança específicas para VOIP. Um sistema de segurança deve poder enxergar dentro do fluxo de VOIP, analisar o estado da ligação e verificar o conteúdo do serviço, certificando-se de que todos os parâmetros estejam coerentes com suas necessidades comerciais.

17.1. Segurança Física dos Componentes e Dispositivos

Sugere-se que a qualidade deste serviço, siga os seguintes critérios:

Para atender a demanda como uma condição prévia para a utilização de diferentes protocolos e equipamentos VOIP a partir de diferentes fornecedores podem tanto ser a favor da emissão de opiniões, têm objeções.Para garantir que os equipamentos selecionados para atender às suas necessidades, mudar os requisitos para dar suporte a equipamentos de um fornecedor específico é um comportamento muito perigoso.

Acordo de parar de usar número desnecessário de acordos muitas vezes são desconhecidos vulnerabilidades sejam exploradas. Não é necessário para permitir que os protocolos desnecessários e não utilizados e dos serviços, proporcionar mais oportunidades para os hackers.

VOIP de autenticação para o terminal de operação remota pode ser atualizado remotamente e gestão. Certifique-se de usar apenas os endereços IP baseados no nome de usuário somente. Finalmente, o que é necessário é um programa de serviços de gerenciamento remoto.

Para separar a rede interna, serviços de VOIP e equipamento de segurança, existe vários sinalização VOIP pode não ser totalmente comando operacional.Portanto, eles podem abrir a porta de comunicação dinâmica, a rede vulnerável a ataques de bounce. Isso faz com que o atacante penetre na LAN interna doutros componentes chaves de negócios. Ao mesmo tempo, devemos utilizar uma separação física ou lógica para VOIP e infraestrutura baseada em IP ultras separados.

O sistema VOIP pode verificar o sistema de segurança deve ser capaz de rever tal tipo de sistema de fluxo de VOIP, análise e inspeção chamada de estado para garantir que todos os parâmetros são os mesmos.

Além das questões acima, também deve considerar o *Network Address Translation* (NAT) sobre o impacto do tráfego VOIP.

Assegurar a gestão da infraestrutura VOIP, porque cada componente é tão fácil como o acesso a qualquer computador, são susceptíveis de ataque. Mesmo os telefones e terminais, todos os sistemas de VOIP são baseados no hardware para executar o software de sistema, tenha certeza que para gerir o sistema operacional básico VOIP.

Por fim, se a realização de VOIP, a segurança é a necessidade de considerar questões importantes, porque o VOIP no mesmo computador como cada nó está acessível.VOIP vulnerável a ataques DoS e *hacking* irá resultar na passagem de chamadas gratuitas não autorizadas, monitoração de chamadas e redirecionamento de chamadas indesejadas e assim por diante.

O sistema VOIP, também traz alguns dos desafios específicos de segurança. Por exemplo, as chamadas de VOIP devem ser de duas partes (informações, ligue para a instalação e a real chamada fluxo de mídia) para análise. Na verdade, relatados só no ano de 2009, o número de incidentes de segurança relacionadas ao VOIP é maior do que o registrado para todos os anos antes de 2004.

17.1.1. Hardware

Baseado nas informações contidas no desenvolvimento desta monografia, a segurança do equipamento está configurada para funcionar com tráfego VOIP e segundo Lawrence, (2009), sugere-se tal ferramenta devido a Nortel Networks ser o

único fabricante norte-americano de IP PBX que comercializa um firewall pré-configurado para funcionar com tráfego VOIP.

> "Tal evidencia a ausência de maturidade do mercado: apenas um fabricante adaptou os passos para que tal acontecesse", refere. (Beraldo, Fabio, 2010)

Na medida em que as competências VOIP ainda são uma especialidade emergente, é preferível que sejam os fabricantes a pré-configurarem estes produtos para funcionarem em conjunto do que contratar um consultor externo para fazer.

17.1.2. Segurança dos Acessos

Este é o principal problema que apresenta hoje em dia a penetração tanto de VOIP como de todas as aplicações de IP. Garantir a qualidade de serviço sobre Internet, que só suporta "melhor esforço" (*best effort*) e pode ter limitações de largo de banda na rota, atualmente não é possível; por isso, sugere-se que se atente quando se apresentam diversos problemas quanto a garantir a qualidade do serviço.

17.1.3. Característica da Criptografia no Serviço VOIP

Estes produtos também disponibilizam outras funcionalidades, como encriptação e autenticação do tráfego de voz. Tais funcionalidades são particularmente importantes se uma organização está a planear executar tráfego VOIP através da Internet.

Portanto seguindo as informações anteriores, sugiro que os clientes devem determinar a complexidade da configuração destas funcionalidades em qualquer serviço VOIP. Embora a ameaça de sistemas de VOIP em uma fase inicial, no entanto, as empresas devem se concentrar em questões emergentes. Firewall e sistemas de prevenção de intrusões geralmente oferecem a melhor proteção.

A maior ameaça é alguém que quando você alterna um ataque de negação de serviço. Você tem a chave localizada atrás de um firewall. Mais de um firewall, também devem ser implementados no protocolo de um equipamento de filtragem de telefonia IP.

17.1.4. Segurança dos Tráfegos de Informação / Protocolos Seguros

Existem vários protocolos VOIP. Segunda a revista RTI,(2009), especialistas em VOIP podem advogar protocolos diferentes, pois estes protocolos têm vantagens, mas a questão da segurança para a maioria dos protocolos VOIP, sugiro que seja visto várias coisas que precisam trabalhar juntos para considerar: a melhor utilização de recomendações de segurança adicionais para eliminar riscos e ataques.

Os sistemas de infraestrutura de PBX VOIP precisam ser adicionados, *gateway, proxy*, registro e servidor de localização para a rede *backbone* IP e telefone. Cada componente de uma rede VOIP, os dados são os mesmos que o outro computador é endereçável e acessível, segundo Beraldo, Fabio, (2010)

Cada componente inclui um processador de VOIP e executar o software podem sofrer ataques de pilha TCP / IP. Ataques à comunicações de dados podem ser realizados por infraestrutura IP de voz. Componentes vulneráveis a ataques de negação de serviço em VOIP vai usar uma falsa voz de congestionamento da rede de comunicações, reduzindo o desempenho da rede ou a cessação de comunicações de voz e dados.

Além disso, se o PC infectado com o pacote de comunicações interceptadas, *Trojans* LAN, baseado em PC *softphone* será muito vulnerável à espionagem. Como sugestão a vulnerabilidades VOIP também pode ser usado para a DMZ (zona desmilitarizada) no servidor e host para lançar ataques de *bounce*.

Em resumo, VOIP permite comunicação de voz e comunicações de dados face a ameaças de segurança mesmo. Ao mesmo tempo, o VOIP também trouxe uma série de desafios de segurança. VOIP telefonema tem dois componentes - a troca da instalação de sinalização de informação e transmissão da "voz" fluxo de mídia.Sinalização e caminhos de mídia são separados, você precisará usar o VOIP para se comunicar a conexão lógica entre as duas partes.

O próprio regular define três elementos fundamentais em sua estrutura:

Terminais: são os substitutos dos atuais telefones. Podem-se implementar tanto em software como em hardware.

Gatekeepers: são o centro de toda a organização VOIP, e seriam o substituto para as atuais centrais. Normalmente implementadas em software, em caso de existir, todas as comunicações passariam por ele.

Gateways: trata-se do enlace com a rede telefônica tradicional, atua de forma transparente para o utente. Com estes três elementos, a estrutura da rede VOIP poderia ser a conexão de duas delegações de uma mesma empresa.

A vantagem é imediata: todas as comunicações entre as delegações são completamente gratuitas. Este mesmo esquema poder-se-ia aplicar para provedores, como conseguinte poupança que isto implica.

Protocolos de VOIP: são as linguagens que utilizarão os diferentes dispositivos VOIP para sua conexão. Esta parte é importante já que dela dependerá a eficácia e a complexidade da comunicação.

A seguir se sugere alguns protocolos de melhor utilização

H323 - Protocolo definido pela ITU-T;

SIP - Protocolo definido pela IETF;

Megaco (Também conhecido como H.248) e MGCP - Protocolos de controle;

Skinny Client Controle Protocol - Protocolo propriedade de Cisco ;

MiNet - Protocolo propriedade de Mitel;

CorNet-IP - Protocolo propriedade de Siemens ;

IAX - Protocolo original para a comunicação entre PBXs Asterisk (É um regular para os demais sistemas de comunicações de dados,[cita requerida] atualmente está em sua versão 2, IAX2);

Skype - Protocolo proprietário peer-to-peer utilizado na aplicação Skype;

Jingle - Protocolo aberto utilizado em tecnologia Jabber;

MGCP- Protocolo proprietário de Cisco ;

WeSIP- Protocolo licencia gratuita de VozTelecom.

17.2. Segurança Lógica

Sugere-se tal como acontece com o qualquer outra tecnologia, um bom firewall e VPN é necessária. No entanto, o firewall e VPN não protege contra todos os tipos de ataque, por isso para o uma segurança em serviço VOIP, deve-se levar essa característica em conta, segundo a Revista oficina net, (2008).

17.2.1. Aplicações de Segurança Lógica

Como sugestão, as aplicações VOIP disponibilizam segurança adequada, como administração multinível em que o acesso às funcionalidades de gestão não está autorizado aos administradores quando tal não for necessário. Por exemplo, uma aplicação deverá ter condições de permitir a um administrador gerir os direitos dos utilizadores e a outro administrador gerir os planos de chamadas sem ter que expor todos os direitos a todos os gestores.

À medida que as instalações VOIP se multiplicam nos ambientes corporativos, também os produtos que tornam seguras as comunicações.

17.3. Aspectos Lógicos

Em muitos países do mundo, IP tem gerado múltiplas discórdias, entre o territorial e o legal sobre esta tecnologia, está claro e deve ficar em claro que a tecnologia de VOIP não é um serviço como tal, senão uma tecnologia que usa o Protocolo de Internet (IP) através da qual se comprimem e descompactam de maneira altamente eficiente pacotes de dados ou datagramas, para permitir a comunicação de duas ou mais clientes através de uma rede como a rede de Internet. Com esta tecnologia podem prestar-se serviços de Telefonia ou Videoconferência, entre outros segundo Beraldo, Fabio, (2010).

17.3.1. Políticas de Segurança

Definido em 1996 pela *UTI* (União Internacional de Telecomunicações) proporciona aos diversos fabricantes uma série de normas com o fim de que possam evoluir em conjunto.

Os produtos de segurança VOIP incluem firewalls, sistemas de prevenção de intrusão, controladores de limites de sessão e outros equipamentos desenhados para proteger a rede de comunicações de voz que transportam tráfego IP das organizações empresariais. Normalmente disponibilizadas como equipamentos, estes produtos tem como objetivo disponibilizar segurança quando os protocolos VOIP não possuem condições.

À semelhança do ambiente de dados, um conjunto de equipamentos de segurança, preocupações e boas práticas são essenciais para implementar com segurança tecnologias VOIP. Estes produtos defendem as redes de voz de ameaças que podem ser vírus, spam ou outro *malware* até ataques de negação de serviço (DoS), intrusão, fraude e roubo.

A segurança do tráfego VOIP torna-se particularmente importante quando uma organização amplia a utilização de telefonia IP para lá dos limites da sua rede de comunicações. Assim que o tráfego de voz viaja na Internet, as precauções como: encriptação e autenticação, tornam-se essenciais.

Atualmente as organizações estão adotando soluções VOIP principalmente para a redução de custos. Mas para uma implementação de VOIP bem sucedida é preciso planejar a segurança do ambiente. A utilização de tradução de endereços de rede (NAT) pode diminuir os investimentos mas também a capacidade de inspecionar o protocolo VOIP abrindo a rede para possíveis ataques.

Contanto com a longa experiência de empresas em telefonia e VOIP, algumas desenvolveram uma solução que permite manter a qualidade do serviço VOIP, mantendo a segurança da rede corporativa e se integrando a várias soluções e protocolos VOIP existentes, uma delas é *Compugraf*, onde desenvolve uma solução que permite manter a qualidade do serviço VOIP, mantendo a segurança da rede corporativa e se integrando a várias soluções e protocolos VOIP existentes.

Os acessos, segundo a Microsoft.com, (2010), você não precisa nem ter um computador para conectar-se a uma rede VOIP. No entanto, à medida que os serviços tornam-se mais comuns, ele atrai a atenção de invasores online e fraudadores. No item 11.5.1 é mostrado os benefícios e desvantagens e as etapas a seguir para aumentar sua segurança para seu próprio uso.

Portanto sugiro acessar o VOIP online, armazenar suas conversas no computador e ouvi-las novamente sempre que desejar, portanto em resumo se você está recebendo ou enviando algum dado, arquivo, foto no seu computador ou na rede de computadores em que a sua linha VOIP também está conectada, a voz ficará em segundo plano nesse momento, poderá então haver perda na qualidade ou interrupção do som principalmente ao falar, ou seja, sua voz chegará ao destino com falhas ou simplesmente será interrompida.

Para quem usa o *softfone* (discador VOIP) no computador somente o aumento da banda poderá solucionar o problema que é a falta de "largura" para o trânsito de dados e voz simultâneos.

Por fim, vale observar que quando você usa o VOIP no seu computador (isolado ou numa rede) a voz não tem prioridade sobre a remessa ou recepção de dados o que dependendo da velocidade ou banda de sua Internet poderá não haver qualidade suficiente para o diálogo na ligação VOIP.

Segundo a Anatel, (2010), o sistema está inserido dentro de licenças SCM (Serviço de Comunicação Multimídia) engloba voz, dados e imagens, licença que algumas empresas que trabalham com esse tipo de tecnologia possui junto a ANATEL para todo território nacional na prestação de serviços deste tipo de tecnologia**.**

A popularização de novas tecnologias é sempre acompanhada por ações de piratas virtuais, que buscam novas alternativas para ganhar dinheiro fácil. Seguindo esta tendência, golpistas criaram novas táticas pra roubar senhas em diversas redes bancárias utilizando a VOIP, tecnologia de voz sobre IP popularizada pelos softwares gratuitos.

Segundo o Beraldo, Fabio, (2010), sugere-se o gerenciamento de senhas, permissões e privilégios, pois a única identificação que um usuário VOIP tem é o número de seu telefone e uma eventual senha para acesso ao serviço. A senha deverá ser armazenada tanto no cliente quanto no servidor. Se as senhas do servidor não tiverem num formato que possam ser revertidas, qualquer usuário com acesso a esse servidor pode obter o nome de usuário e a senha referente a ele, portanto se atente a escolher um bom.

Por fim, o site microsoft.com, indica, mantenha senhas fortes e particulares: crie senhas fortes para acessar os sites de serviços na Web que armazenam seu correio de voz e outros dados de áudio.

Não compartilhe essas senhas, instale acesso direto e remoto à rede VOIP e mantenha todo o software de sistema operacional atualizado. Além disso, você deve proteger por senha e criptografar, quando possível, qualquer rede sem fio utilizada. Isso também se aplica a *Smartphones* e a qualquer outro dispositivo de transmissão de dados sem fio; eles também podem ser alvos de ataque online.

A figura 16, mostra uma janela para conexão através de senha.

Figura 16 - Janela para conexão através de senha. Fonte:baboo (2009)

18. Projetos Futuros

A tecnologia VOIP também tem sido aplicada em PABX (***P**rivate **A**utomatic **B**ranch **E**xchange*), os conhecidos sistemas de ramais telefônicos. Dessa forma, muitas empresas estão deixando de ter gastos com centrais telefônicas por substituírem estas por sistemas VOIP.

A tecnologia VOIP dessa maneira, muitas empresas estão deixando os gastos com centrais telefônicas e também os gastos e substituindo pelo referida tecnologia.

Movimentos que estimulam a convergência estão transformando a cadeia de valor nos mercados de comunicação que antes eram realizadas a difusão por diferentes

meios de transmissão e estão sendo unificados e transmitidos em um único meio a telefonia, os dados, a música e televisão.

A banda larga, a velocidade de banda é o diferencial competitivo. Tecnologia, capacidade de transmissão, capacidade de processamento, compressão de dados, capacidade de armazenamento, novos dispositivos para clientes.

Consumidores novas demandas, internet de alta velocidade, interatividade, provedor único, mobilidade, dispositivos integrados, acesso ao conhecimento/educação, são campos onde esta tecnologia poderão ser serem aplicadas.

Sugiro para um VOIP seguro, segundo Beraldo, Fabio (2010):

· Priorização da segurança, sem negligenciar a qualidade de serviço nem a funcionalidade

· Confiança no funcionamento é justificada pela análise e pela mitigação dos riscos de maior preocupação para a organização.

18.1. O Futuro do Serviço VOIP

Pelos projetos atuais das empresas que hoje trabalham com VOIP, segundo analistas de mercado e alguns pontos de opinião, uma das próximas etapas na evolução do VOIP é a extinção por completo do modelo atual de ligações de longa distância (DDD/DDI) pela rede PSTN e, mais adiante, talvez a erradicação dos sistemas convencionais de telefonia.

Parte desta evolução estará à medida que os telefones IP chegarem aos lares e os acessos em banda larga se popularizarem. Neste sentido, vários segmentos trabalham no intuito de criarem redes convergentes, seja utilizando os meios de transmissão telefônica atual, já compartilhado por serviços ADSL, seja compartilhando meios de transmissão de serviços de televisão a cabo, entre outros.

O futuro da tecnologia VOIP são as comunicações unificadas (UCOIP) (*Unified Communication over IP*).

19. Conclusão

O serviço VOIP está mudando as comunicações, reduzindo o seu custo e simplificando a infraestrutura das empresas. Com a previsão de aumento no uso de VOIP, é provável que os invasores busquem cada vez mais formas de explorar essa tecnologia, que por sua vez já está sujeita à maioria das ameaças que colocam em risco as redes de dados.

Se a sua empresa optar por adotar VOIP, ela deverá estar preparada para lidar com a falta de recursos de segurança que estão integrados nos sistemas VOIP atuais. Com consciência e compromisso com a segurança, sua empresa pode tirar proveito da redução de custos que a VOIP oferece.

Conforme o modelo de proposta de serviço VOIP, para compor solução de integração do Sistema de Telefonia de órgãos e entidades da Administração Pública, compreendendo fornecimento, instalação, ativação, transferência de tecnologia e garantia de funcionamento, pode-se ser uma referência para aplicações futuras na implementação de infraestrutura VOIP.

Avançar tecnologicamente não é uma alternativa, a história comprova que não renovar suas capacidades e infraestrutura é caminho certo para o fracasso. Grandes avanços foram implementados desde a invenção do telefone e salvo por alguma questão cultural, não encontraremos um telefone de manivela em uma empresa de sucesso.

A tecnologia VOIP é um avanço tecnológico em telecomunicações, os custos – benefícios são bem atrativos, uso de protocolos padronizados garantem a interoperabilidades e, é um elemento motivador para empreendimentos futuros, garantindo assim ser uma tecnologia do momento.

Por fim, gostaria de agradecer aos professores e os futuros pós-graduados da turma de Segurança da Informação da Faculdade UNEB, já profissionais, pelos longos períodos de estudos e dedicação, pelas turbulentas discussões e ajuda na elaboração desta monografia.

Referências Bibliográficas

BASET, Salman A., SCHULZRINNE, Henning (15 de setembro de 2004). An Analysis of the Skype Peer-to-Peer Internet Telefhony Protocol;

BERALDO, Fabio - Revista TI, Tecnologia em Voip, (2010);

BATISTA, Jéssica – Segredo do sucesso - Edição 15, Ano 3 (2011);
Caderno de Pós-Graduação – Administração, São Paulo, v.4, n.1, especial, RAI, p. 413-423, 2005, acessado em 24 de dezembro de (2010);

LAWRENCE – Tecnologia voip, (2009);

PAGANUCHI, Alessandro do CPqD, 20 de outubro de (2008);

DAVIDSON - Fundamentos de Voip - 2ª EDIÇÃO, (2010);
MOHER, Michael - Sistemas de comunicação – 5ª edição (2011);

REVISTA RTI – Redes, Telecom e Instalações/ ARANDA editora – Ano XI, nº 123 – Agosto de (2010);

ANDERSON, Eric – Protocolos e sistemas voip, (2009);

REVISTA, Revista oficina net, (2008)

Sites para referências:

MICROSOFT.COM, sistemas voip - acessado em dezembro (2010);

http://www.mcafee.com - acessado em 24 de dezembro de (2010);

http://www.ipnews.com.br/seguranca-em-voip-acessado em 12 de novembro de 2010;

http://www.Sisco, Sistemas voip, (2009);

http://www.ipnews.com.br/voip/infra-estrutura/banda-larga-em 15 de janeiro de (2011);

http://www.computerworld.com.pt/2010, acessado em 10 dezembro de (2010);

http://www.teleco.com.br/, acessado em 15 de janeiro de (2011);

http://voipequipamentos, (2010);

http://www.icatel.com.br/voip.asp, acessado em 10 de fevereiro de (2011);

http://www.siemens, (2010);